2022-12

IDENTIFYING OPPORTUNITIES TO ALIGN U.S. AIR FORCE AND U.S. ARMY MULTI-DOMAIN OPERATIONS IN THE CONTEXT OF INTEGRATED DETERRENCE: AN ANNOTATED BIBLIOGRAPHY OF DETERRENCE AND MULTI-DOMAIN OPERATIONS

Stelmack, Robert A.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DEFENSE ANALYSIS CAPSTONE REPORT

IDENTIFYING OPPORTUNITIES TO ALIGN U.S. AIR FORCE AND U.S. ARMY MULTI-DOMAIN OPERATIONS IN THE CONTEXT OF INTEGRATED DETERRENCE: AN ANNOTATED BIBLIOGRAPHY OF DETERRENCE AND MULTI-DOMAIN OPERATIONS

by

Robert A. Stelmack

December 2022

Thesis Advisor: Kalev I. Sepp
Second Reader: Cecilia Panella

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Defense Analysis Capstone Report

4. TITLE AND SUBTITLE
IDENTIFYING OPPORTUNITIES TO ALIGN U.S. AIR FORCE AND U.S. ARMY MULTI-DOMAIN OPERATIONS IN THE CONTEXT OF INTEGRATED DETERRENCE: AN ANNOTATED BIBLIOGRAPHY OF DETERRENCE AND MULTI-DOMAIN OPERATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Robert A. Stelmack

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The objective of this capstone is to identify readings that can suggest doctrinal changes to better align U.S. Army and U.S. Air Force concepts of multi-domain operations. Currently, there is no joint consensus on how to conceptualize multi-domain operations or how they should support the 2022 *National Security Strategy.* This capstone identifies readings related to two areas of potential alignment between U.S. Army and U.S. Air Force doctrine: Deterrence Theories and Multi-Domain Operations. It also suggests designating service leads for long-range fires and command and control, and furthering development of common technological standards. Future research could study the readings identified in this capstone to refine and develop multi-domain operations doctrine.

14. SUBJECT TERMS
multi-domain operations, cross-domain deterrence, information warfare, combined joint all-domain operations

15. NUMBER OF PAGES
105

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

IDENTIFYING OPPORTUNITIES TO ALIGN U.S. AIR FORCE AND U.S. ARMY MULTI-DOMAIN OPERATIONS IN THE CONTEXT OF INTEGRATED DETERRENCE: AN ANNOTATED BIBLIOGRAPHY OF DETERRENCE AND MULTI-DOMAIN OPERATIONS

Robert A. Stelmack
Captain, United States Air Force
BS, United States Air Force Academy, 2017

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED DESIGN FOR INNOVATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Kalev I. Sepp
Advisor

Cecilia Panella
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The objective of this capstone is to identify readings that can suggest doctrinal changes to better align U.S. Army and U.S. Air Force concepts of multi-domain operations. Currently, there is no joint consensus on how to conceptualize multi-domain operations or how they should support the 2022 *National Security Strategy*. This capstone identifies readings related to two areas of potential alignment between U.S. Army and U.S. Air Force doctrine: Deterrence Theories and Multi-Domain Operations. It also suggests designating service leads for long-range fires and command and control, and furthering development of common technological standards. Future research could study the readings identified in this capstone to refine and develop multi-domain operations doctrine.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

A2/AD	Anti-Access/Area Denial
ABMS	Air Battle Management System
ARSOF	Army Special Operations Forces
CJADC2	Combined Joint All-Domain Command and Control
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
DOD	Department of Defense
DoDI	Department of Defense Instruction
EW	Electronic Warfare
IC	Intelligence Community
IO	Information Operations
IOT	Internet-of-Things
IW	Information Warfare
JADC2	Joint All-Domain Command and Control
JADO	Joint All-Domain Operations
MISO	Military Information Support Operations
NDAA	National Defense Authorization Act
NPS	Naval Postgraduate School
NSS	National Security Strategy
NSS	National Security Strategy
OIE	Operations in the Information Environment
PRC	People's Republic of China
PSYOP	Psychological Operations
SIO	Special Information Operations
SOF	Special Operations Forces
US	United States
USAF	United States Air Force
USAFRICOM	United States Africa Command

USASOC	United States Army Special Operations Command
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USEUCOM	United States European Command
USFLEETCYBER	United States Fleet Cyber Command
USINDOPACOM	United States IndoPacific Command
USNORTHCOM	United States Northern Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command

EXECUTIVE SUMMARY

The objective of this capstone is to identify readings that can suggest doctrinal changes to better align U.S. Army and U.S. Air Force (USAF) concepts of multi-domain operations. Currently, there is no joint consensus on how to conceptualize multi-domain operations despite its emphasis within each service. Furthermore, no concept of multi-domain operations in relation to integrated deterrence is described in the *2022 National Security Strategy*'s (NSS). This capstone supports rectifying these issues by identifying resources that future doctrine writers may study to better align service concepts of multi-domain operations while supporting the 2022 NSS and integrated deterrence.

This capstone suggests two areas of potential alignment between U.S. Army and USAF multi-domain operations doctrine: designating service leads for long-range fires and command and control and developing technological standards. Each area can be informed through the readings this capstone analyzes. These areas of potential alignment may enable multi-domain operations to meet requirements and objectives of the 2022 NSS.

This capstone suggests that despite both the U.S. Army and USAF having their own conceptions of multi-domain operations, they are internally consistent. The main theme of U.S. Army multi-domain operations is long-range fires, while the unique key tenet for USAF multi-domain operations is command and control. Future multi-domain operations doctrines could be better aligned by designating service leads based on these key concepts. By doing so, each service will gain more responsibility in their investments in capability and skill while sacrificing control over the other key tenet. In addition to these unique key tenets, both service concepts include the key tenets of influencing populations and integrating non-kinetic fires. Despite these suggestions for alignment, it is important to remember that multi-domain operations are too young and too broad to designate an appropriate service lead for full integration.

Both U.S. Army and USAF multi-domain operations place significant weight on a technological backbone. However, both services are simultaneously developing distinct technological programs to support their doctrines. Future research may benefit from one

service being selected as the lead for standardizing and developing this technology. In turn, both services' concepts of multi-domain operations would increase in efficiency and interoperability.

Future research based on this capstone should study the identified readings and attempt to align U.S. Army and USAF doctrines based on the two areas previously outlined. Doing so may result in a joint force more capable of operating coherently and more likely to succeed in deterring adversary operations.

ACKNOWLEDGMENTS

I would like to thank all of the professors in the Defense Analysis Department and at the Naval Postgraduate School for their time, expertise, and insightful discussions. Without you, my NPS experience would not have been nearly as rewarding. Further, I would like to thank Dr. Kalev Sepp and Cecilia Panella for their continued support in writing this capstone. Finally, I would like to thank my friends and family for enduring tireless hours of capstone-related conversation.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The United States (U.S.) Department of Defense (DOD) is currently transitioning between a focus on global counter-violent extremist organization operations and countering the "growing multi-domain threat posed by the [People's Republic of China (PRC)]."[1] In an April 2021 speech, Secretary of Defense Lloyd Austin named the DOD's strategy for deterring that threat "integrated deterrence."[2] The 2022 *National Security Strategy* (NSS) now defines integrated deterrence as the "seamless combination of capabilities to convince potential adversaries that the costs of their hostile activities outweigh their benefits" through integration across domains, regions, the spectrum of conflict, the U.S. government, and with allies and partners.[3] Despite this high-level guidance, it is still not widely understood what exactly integrated deterrence will entail, or how it will differ from previous deterrence strategies.

Although the NSS has defined integrated deterrence, it has not provided more granular guidance on how to successfully execute this strategy. One way for operational-level entities to overcome this unknown is through the application of deterrence theories in accordance with commander's guidance. While older deterrence theories are not expected to be entirely applicable, they may still have relevance to today's problem sets. Newer deterrence theories, such as cross-domain deterrence, may present more innovative solutions for achieving integrated deterrence. An exploration of deterrence theories would provide greater insight into how integrated deterrence can develop from high-level guidance to more specific directions.

Integrated deterrence has come into use simultaneously with the Department of Defense's concept of multi-domain operations. "Multi-domain operations" refers to an overarching, multi-service initiative that describes how the services plan to compete and

[1] White House, *National Security Strategy*, October 2022 (Washington, DC: White House, 2022), 22.

[2] Lloyd Austin, "Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command," Speech. April 2021. https://www.defense.gov/News/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/

[3] White House, National Security Strategy, 22.

win against adversaries in the future. The initiative is an evolution of prior ideas such as the Third Offset Strategy, Airland Battle, and Multi-domain Battle. Each service has also developed its own technological component related to multi-domain operations, such as the U.S. Army's Project Convergence or the U.S. Air Force's (USAF) Air Battle Management System (ABMS).[4] Today, doctrine on the expansive initiative accounts for military operations across all domains, stages of competition, and allies and partners.

Despite the near decade of development, the initiative has no common definition at the joint level. Both the U.S. Army and USAF have developed their own internally cohesive versions of multi-domain operations. In order for multi-domain operations to be successful as a joint operational concept, a common understanding of the initiative must exist. Furthermore, any common understanding of the initiative must be tied to the current NSS' priority of integrated deterrence. To date, no academic research exists which aligns integrated deterrence with multi-domain operations. The lack of integrated deterrence's specificity and a common understanding of multi-domain operations leaves two of the DOD's largest initiatives largely unreconciled.

A. RESEARCH OBJECTIVE

The purpose of this capstone is to identify readings that can suggest doctrinal changes to better align USAF and U.S. Army concepts of multi-domain operations. This objective is significant as there exists a litany of confusing, unspecific, and contradictory information surrounding the topics. Bringing clarity to these topics will bolster future research opportunities focused on developing compatible multi-domain operations concepts.

[4] Yasmin Tadjdeh, "Navy Dedicates More Resources To Secretive Project Overmatch," *National Defense* (August 2021). https://www.nationaldefensemagazine.org/articles/2021/8/10/navy-dedicates-more-resources-to-secretive-project-overmatch

B. APPROACH

This capstone takes the form of an annotated bibliography. The capstone reviews the most significant material pertaining to deterrence and multi-domain operations in order to achieve the research objective.

C. ORGANIZATION

This capstone is organized into three categories: deterrence, multi-domain operations, and related research. The deterrence portion of the capstone covers various theories such as conventional deterrence, nuclear deterrence, and cross-domain deterrence. Next, the multi-domain operations portion of the capstone reviews primarily U.S. Army and USAF multi-domain operations through both academic scholarship and the writings of practitioners. Finally, the last section of this capstone focuses on related research conducted while the capstone was produced. The capstone concludes by discussing two possibilities for aligning U.S. Army and USAF multi-domain operations doctrine. This capstone includes in the appendix multiple works published or created by the author during the research process.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DETERRENCE READINGS

This chapter focuses on reviewing the topic of deterrence as contextualization for integrated deterrence as defined in the NSS 2022. It begins by reviewing potentially relevant discussions on deterrence-related scholarship including political realism, international relations, and deterrence theories. Next, it analyzes several deterrence theories including conventional deterrence, nuclear deterrence, and cross-domain deterrence. It summarizes that while ample research exists on deterrence theory, the most applicable theory for multi-domain operations is cross-domain deterrence. Future multi-domain operations doctrine may be able to align how they integrate deterrence theory as an overarching theme.

A. DISCUSSIONS ON DETERRENCE

The History of the Peloponnesian War is Thucydides's quintessential work where he describes the Peloponnesian War from 431–404 BC. Although Thucydides was an Athenian general, academics consider his documentation of the Athenian and Spartan wars an accurate and unbiased one. Today his historical account serves as evidence for a vast array of writings on political theory, to include much of Political Realism and, by extension, deterrence.[5]

Politics Among Nations: The Struggle for Power and Peace is a classic book that has formed the basis of Western political science. Written by Dr. Hans Morgenthau in 1948, the book describes the interaction of states through an understanding of their pursuit for power.[6] The "struggle for power and peace" in this book is foundational for understanding using power to influence the decisions of state actors.

Dr. Kenneth Waltz's work *Theory of International Politics*, like Dr. Morgenthau's, is essential to today's study of Political Realism. Two of the most common interpretations

[5] Thucydides, *The History of the Peloponnesian War*, trans. Richard Crawley (New York: E. P. Dutton and Company, Inc., 1950), 1.

[6] Hans Morgenthau, Politics Among Nations: The Struggle for Power and Peace (New York: Knopf, 1954), 4.

of Waltz's work have ramifications for this capstone. First, that the international system is anarchic, and defined by the absence of a "higher authority."[7] Second, that the distribution of power amongst nations defines the state of the international system. These observations are important to this capstone as they form the underlying basis for deterrence theory.

In Chapter 4 of his book *After Hegemony: Cooperation and Discord in the World Political Economy*, Dr. Robert Keohane describes the interaction of cooperation and international regimes. Dr. Keohane develops a model to distinguish between harmony, cooperation, and discord based on actions between states. For the purposes of this capstone, most useful is his analysis which informs how states can cooperate without necessarily being harmonious.[8]

"Thucydides and Neorealism" by Dr. Daniel Garst is a criticism and rebuking of Neorealist writings which cite *The Peloponnesian War* as the basis of their thought. Dr. Garst both combats the Neorealist interpretation of Thucydides's writings and continues on to criticize Neorealism as a whole. He concludes that Thucydides's writings indicate a far greater utility for Liberalism than Neorealism.[9] His argument is that Political Realists have misinterpreted the writings of Thucydides and by extension, misunderstood the role hegemony played during the Peloponnesian War.[10] He writes that Political Realists therefore misunderstand the role of political power and its relationship to hegemony.[11] Dr. Garst' s critique invites caution on relying too heavily on Political Realism when discussing deterrence.

Dr. Michael Doyle in "Thucydidean Realism" compares and contrasts the Political Realist variants of Structuralist, Fundamentalist, and Minimalist to determine which branch is most directly supported by Thucydides's writing. Through this comparison, he

---

[7] Kenneth Waltz, *Theory of International Politics* (Mass: Addison-Wesley, 1979).

[8] Robert Keohane, "Cooperation and International Regimes," in *After Hegemony: Cooperation and Discord in the World Political Economy* (NJ: Princeton University Press, 1984).

[9] Daniel Garst, "Thucydides and Neorealism," International Studies Quarterly 33, no. 1 (1989): 3–27. https://doi.org/10.2307/2600491.

[10] Garst.

[11] Garst.

eventually concludes that to be "Thucydidean" means to "see that states are not structurally equivalent and that the differences are consequential."[12] Therefore, any conclusions this capstone draws based upon Political Realism should account for a states' structural organization.

In "The Use and Abuse of Thucydides in International Relations" by Dr. Laurie Johnson Bagby, she argues that Political Realism relies too heavily on historical writings such as Thucydides's to develop their political theories. She recommends that future political theorists use caution in attempting to distill deterministic theories about the actions of mankind, to include international relations. This is a useful viewpoint that demonstrates the limited value of theoretical modeling versus applied experimentation.[13]

Dr. John Herz describes the "security dilemma" in "Political Ideas and Political Reality." This dilemma serves as a bedrock component of Political Realism and describes the phenomena of one state's pursuit of security encouraging another state's pursuit of security and, paradoxically, reducing the first state's security in the process. Through an analysis of the socio-political connection between man and security, he concludes a "predominance of the security urge between men and groups."[14] He also concludes that this condition may not be "eternal," and policies may be able to account for this phenomenon.

In "Deterrence Theory Revisited" by Dr. Robert Jervis, he reviews the "three waves" of deterrence theory as they existed in 1979.[15] The first theory is composed of "scholars such as Bernard Brodie, Arnold Wolfers, and Jacob Viner" who wrote in the aftermath of World War II.[16] Although they were "amazingly quick to see the implications

---

[12] Michael Doyle, "Thucydidean Realism," *Review of International Studies* 16, no. 3 (1990): 223–37. http://www.jstor.org/stable/20097224.

[13] Laurie M. Johnson Bagby, "The Use and Abuse of Thucydides in International Relations," *International Organization* 48, no. 1 (1994): 131. http://www.jstor.org/stable/2706917.

[14] John Herz. "Political Ideas and Political Reality," *The Western Political Quarterly* 3, no. 2 (1950): 161–78. https://doi.org/10.2307/443481. 161.

[15] Robert Jervis, "Deterrence Theory Revisited," *World Politics* 31, no. 2 (1979): 289. https://doi.org/10.2307/2009945.

[16] Jervis, "Deterrence Theory Revisited," 291.

of nuclear weapons," Dr. Jervis writes, "part of the reason they did not have more influence is that the general and long-run considerations being examined were too far removed from the pressing international problems of the day."[17] He writes that the first wave "had relatively little impact."

The second wave of deterrence theory is described as the contributions of "Schelling, Snyder, Wohlstetter, and others" which often "uses the game of Chicken as an analogy."[18] In describing the second wave, he notes "only the most important [criticisms]" such as its inability to describe "how to change the other's motives," to model rewards versus punishments, and to incorporate the possibility of total irrationality.[19] Given the second wave's impact on later deterrence literature and the situations it does model well, it is worthwhile to review.

The third wave of deterrence theory is defined then as scholarship which writes on "three main difficulties that were not raised by earlier critics [of second wave deterrence theory]."[20] These three difficulties are defined as a lack of using empirical findings, of investigating the impact of the costs of retreat, and of incorporating the goals of policy and politics.[21] Dr. Jervis describes this wave as useful both for continuing to refine theory from the second wave as well as for addressing the growing complexity of the international environment.[22] Dr. Jervis's categorizations may provide a useful framework for understanding Cold War deterrence theory to researchers.

In "Dilemmas About Security Dilemmas," Dr. Robert Jervis reviews Dr. Charles Glaser's work on "wrestling with the security dilemma."[23] This review places Dr. Glaser's work in the context of Political Realism and presents some potential critiques. Dr. Jervis

17 Jervis, 291.

18 Jervis, 291.

19 Jervis, 301.

20 Jervis, 301.

21 Jervis, 323.

22 Jervis, 324.

23 Robert Jervis, "Dilemmas About Security Dilemmas," *Security Studies* 20:3 (2011), 416–423.

concludes that Dr. Glaser's analysis is "rich" in its treatment of international relations but, like Realism, "downplays the importance of domestic politics and ideologies."[24]

Dr. Richard Ashley critiques the then-growing field of Neorealism in his article "The Poverty of Neorealism." In his review, he writes of the emphasis the most well-known "Neorealists" place on objectivity in their work. Dr. Ashley concludes that Neorealists, in attempting to eschew the traditions of Classical Realism and focus more on objectivity, have invalidated their intellectual roots and therefore the legitimacy of their analysis.[25] He further cites the tradition of Political Realism as not needing nor benefiting from this form of objectivity.[26] His criticism highlights the flaws of attempting to distill real-life problems into theoretical models.[27]

Dr. Robert Gilpin rejected Dr. Ashley's critique in his response article "The Richness of the Tradition of Political Realism." Although some of his critiques are more focused in the style of Dr. Ashley's writings, Dr. Gilpin points out that modeling the international system is problematic because of its inherent anarchy.[28] He further discusses that while there are multiple legitimate approaches to understanding the international system, none are inherently more legitimate or objective than the others.[29] Dr. Gilpin concludes that Political Realism is in fact objective and useful for examining the behavior of states despite the various models which exist.[30]

Dr. Michael Webb and Dr. Stephen Krasner in "Hegemonic Stability Theory: An Empirical Assessment" "attempt to assess the empirical validity of the hegemonic stability capstone as an explanation for trends in the international political economy since 1945."[31]

---

[24] Jervis, 416–423.

[25] Richard Ashley, "The Poverty of Neorealism," *International Organization* 38, no. 2 (1984): 230.

[26] Ashley, 231.

[27] Ashley, 228.

[28] Robert Gilpin, "The Richness of the Tradition of Political Realism," *International Organization* 38, no. 2(1984): 287.

[29] Gilpin, 288.

[30] Gilpin, 287.

[31] Michael Webb and Stephen Krasner, "Hegemonic Stability Theory: An Empirical Assessment," *Review of International Studies* 15, no. 2 (1989): 183. http://www.jstor.org/stable/20097178.

To do so, they review hegemonic stability theory as a whole, quantitatively describe the international political economy, and draw their conclusion. This is primarily that hegemonic stability theory is a fair explainer of international relations, but only when it is used to explain security issues.

In *Conventional Deterrence*, Dr. John Mearsheimer uses several case studies to describe how deterrence works in non-nuclear situations, such as the development of German blitzkrieg tactics in World War II. Dr. Mearsheimer's logic examines the various forms and types of deterrence required today given not all of them are nuclear in nature.[32]

Dr. Thomas Schelling describes how "military potential is used to influence other countries, their government or their people, by the harm it could do to them."[33] In *Arms and Influence*, Dr. Schelling describes a variety of ideas related to deterrence including compellence, brinkmanship, and the interplay of tactical and strategic nuclear weapons. Other topics explored include how military power can be used to perform coercion and the relationship between weapon vulnerability and the stability between nuclear-armed states.[34] Dr. Schelling's main argument is that "the threat of damage, or more damage to come" can be used to shape international behavior in a way not possible before.[35] His work is significant in informing deterrence theories throughout the Cold War and today.

In "Cyberpolitics in International Relations," Dr. Nazli Choucri writes on the "conjunction" of politics and cyber.[36] Dr. Choucri writes how the "construction of cyberspace" impacts international relations theory through multiple models which draw on both case studies and policy. The book presents multiple avenues of consideration for integrated deterrence.

---

[32] John Mearsheimer, *Conventional Deterrence* (New York: Cornell University Press, 1983), Preface.

[33] Thomas Schelling, *Arms and Influence*: *With a new Preface and Afterword* (New Haven, CT: Yale University Press, 2008). Xiv.

[34] Schelling, 255.

[35] Schelling, 3.

[36] Nazli Choucri, "Cyberpolitics in International Relations," *Précis* (spring 2013: 6–10, 28.

Dr. Amir Lupovici writes in "Cyber Warfare and Deterrence: Trends and Challenges in Research" on the intersection of deterrence theory and cyberwarfare. He lays out the central claims of deterrence and compares them to factual realities concerning cyberwarfare. He concludes that deterring cyberwarfare through cyberwarfare alone is an inherently tricky task given the asymmetric nature of developing cyber capabilities.[37] This insight is constructive for this capstone, especially concerning the use of multi-domain or cross-domain deterrence strategies.[38]

In "U.S. Cyber Deterrence: Practice Guiding Theory," Dr. Alex Wilner reviews the existing body of literature on deterrence and categorizes it into four distinct phases. Dr. Wilner's analysis includes both actions by state and non-state actors. He concludes that further research should encompass U.S. government activities outside of military coercion, and the academic investigation should be multidisciplinary in nature.[39]

Dr. Thomas Rid and Dr. Ben Buchanan write in "Attributing Cyber Attacks" on the relationship between attribution and state action. Although their publication dedicates attention to tactical and operational attribution, the most impactful finding for this capstone addresses strategic attribution. Dr. Rid and Dr. Buchanan conclude that the use of strategic attribution as a tool of statecraft is dependent upon whether or not any individual state assigns value to their actions being exposed or attributed.[40] For example, attributing an attack to an adversary may not be impactful if that state does not care.[41] This is valuable for understanding how multi-domain actions may have significantly varying deterrent effects depending on the actor being targeted, especially with regards to cyberwarfare.

In "Deterrence, Influence, Cyber Attack, and Cyberwar," Dr. Paul Davis writes on the intersection of "cyberwar" as he defines it and "deterrence within a broader

---

[37] Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs* 3, no. 3 (2011).

[38] Lupovici, 49.

[39] Alex Wilner (2020) "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies,* 43:2, 251.

[40] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2, 7.

[41] Rid and Buchanan, 7.

framework."[42] He continues by creating models that allow for the dynamic application of "rationality" depending on the characteristics of the "state being deterred." Dr. Davis has two key conclusions for this capstone. First, that "cyberwar" should be considered only as cyber within war distinct from a "standalone cyberwar." Second, that deterrence discussions should focus on punishment and that denial should focus on influence separated from deterrence.[43]

Dr. Martin Libicki's *Conquest in Cyberspace* is a well-known work describing the nature of cyber conflict. Dr. Libicki presents "noise tolerance" as a characteristic of information systems and uses his "castle and agora" model to describe the two discrete ends. This model can assist in the understanding of both the nature of cyberspace activities, and also how noise tolerant environments impact deterrence considerations.[44]

Cross-Domain Deterrence: Strategy in an Era of Complexity, an edited volume by Dr. Jon Lindsay and Dr. Erik Gartzke, sets out to "problematize cross-domain deterrence as a theoretical concept."[45] In their introductory chapter to the book, they set the writing's context by tracing deterrence through Thucydides' *History of the Peloponnesian War* to the "George W. Bush administration's attempt" to grapple with deterrence in multiple domains.[46] The introductory chapter provides a solid base for cross-domain deterrence, including a review of anti-access/area denial, air-sea battle, and multi-domain operations. The chapter concludes by summarizing applied topics of cross-domain deterrence.

The chapters of the book cover cross-domain deterrence from strategic and policy implications to more operational considerations. Information on cross-domain deterrence as applied to both the long-range fires key tenet of multi-domain operations and as applied to cyber and information warfare is key to this capstone. Although this chapter does not

[42] Paul Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *International Law and Politics* 47, (2015). 347.

[43] Davis.

[44] Martin Libicki, *Conquest in Cyberspace* (Cambridge: Cambridge University Press, 2007).

[45] Jon Lindsay and Erik Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York, NY: Oxford University Press, 2019).

[46] Jon Lindsay and Erik Gartzke, *Cross-Domain Deterrence*.

tackle the problem of multi-domain command and control directly, it does provide insight into the historical context of both the U.S. Army and USAF multi-domain operations..

"New Challenges in Cross-Domain Deterrence" by Dr. King Mallory is a RAND Corporation Perspective that "examines ways and means by which the United States and its allies might meet these new challenges in cross-domain deterrence."[47] The author performs this examination by elaborating on how the world has changed since academics defined the distinct types of "classic" deterrence. They explain cross-domain deterrence as it pertains to the "space, hybrid warfare, terrorism, and cyberwarfare" domains.[48] Dr. Mallory breaks down deterrence into a list of "alternative strategy sets" across the "degree of force or coercion" as options for U.S. policy makers.

While many academics have attempted to tackle "cross-domain deterrence" or similarly named ideas, Dr. Mallory's writing deconstructs the complex interaction between multiple states of interstate interaction, domain activity, and strategy requirements. For this capstone in particular, the author's attention to "in-domain" and "cross-domain" deterrence in the cyber domain provide insights into MDO that may prove useful for future research. His partitioning of deterrent strategies provides an excellent framework for aligning multi-domain operations.

"Cross Domain Deterrence and Hybrid Conflict" by Dr. Tim Sweijs and Samo Zilincik "reviews the rise of cross domain deterrence in the context of deterrence theory" and applies it to hybrid domains.[49] Although the authors grapple with various definitions, for the purposes of this capstone "hybrid conflict" as used here is synonymous with grey zone operations.[50] The authors focus on the interaction between the ability to deter in the grey zone and the inherent nature of liberal democracies. They conclude that liberal

[47] King Mallory, "New Challenges in Cross-Domain Deterrence," Perspective. (RAND: Santa Monica, CA: 2018).

[48] Mallory, 2.

[49] Tim Sweijs and Samo Zilincik, "Cross Domain Deterrence and Hybrid Conflict," Report. *The Hague Centre for Strategic Studies* (December 2019).

[50] Sweijs and Zilincik.

democracies must develop hybrid capabilities and use them in a proactive nature to deter future grey zone activities.

This writing describes the connection between deterrence and the nature of government ideology. While this capstone does not address deterrence in the context of liberal democracies, it is relevant to consider this context when developing potential roles for multi-domain operations. The manner and method in which a government operates impacts a whole-of-government spanning activity such as integrated deterrence.

In *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression*? by Dr. Timothy Bonds et al.'s objective "was to examine how fielding land-based anti-access/area denial capabilities would affect regional, political, economic, and military dimensions of relations in key regions."[51] The authors use scenarios pertaining to the People's Republic of China as examples for their work, to include potential conflict scenarios involving the Philippines, Republic of Japan, and Republic of Taiwan. The authors' final recommendations are for improvements to multi-domain unit structures, technologies, and integration with foreign partners. In the authors' own words, "A2/AD concepts shift the primary responsibility for defense to U.S. allies and partners."[52] This product aids in understanding multi-domain operations as it pertains to the U.S. Army in the Indo-Pacific theater. In turn, the authors inform this capstone on how to present the delineation between U.S. Army and other service multi-domain operations.

These readings present two common themes that would assist future researchers in aligning multi-domain operations at the joint level. First, early deterrence scholars suggest that deterrence is both structural and theoretical. Any discussion of aligning multi-domain operations should consider the extent to which the structure of the DOD will affect the strategic application of integrated deterrence. Second, future researchers must consider the

---

[51] Timothy M. Bonds, Joel B. Predd, Timothy R. Heath, Michael S. Chase, Michael Johnson, Michael J. Lostumbo, James Bonomo, Muharrem Mane, and Paul S. Steinberg, *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression*?. Santa Monica, CA: RAND Corporation, 2017.

[52] Timothy Bonds et al.

placement and bias of these classical scholars. The majority of these scholars are academics, and future researchers should consider what operational or tactical gaps have been overlooked when looking to better align multi-domain operations for the Department of Defense.

B. DETERRENCE THEORIES

While the 2022 NSS provides a write-up on integrated deterrence, it does not explain how it leverages theory to effectively shape adversary behavior. In the absence of a clearer definition of integrate deterrence, this chapter looks at conventional, nuclear, and cross domain theories and analyzes them for their ability to inform how integrated deterrence can be leveraged to achieve goals listed by the 2022 NSS and inform multi-domain operations doctrine.

1. Conventional Deterrence Theory

Conventional deterrence theory can be used to suggest doctrinal changes to better align U.S. Army and USAF multi-domain operations. This section discusses conventional deterrence's treatment of two topics: deterrence by punishment versus deterrence by denial, and the relationship between Precision Guided Munitions (PGMs) and conventional deterrence. The University of Chicago's Dr. John Mearsheimer focuses on conventional deterrence during the Cold War. He explores the question "why do nations faced with the prospect of large-scale conventional war decide to attack in some cases but not in others?"[53] To make his case, he selects various case studies from the Second World War and the Arab-Israeli conflicts to develop his idea.[54]

Conventional deterrence is appropriate for informing multi-domain operations doctrine given its natural fit for strategic competition. On this subject, Dr. Robert Haffa writes that "reinforcing the logic of conventional deterrence on [the United States'] would-be adversaries should be a central concept of U.S. defense policy over the next decade or

[53] Mearsheimer, Preface.

[54] Mearsheimer, Preface.

so."[55] A retired USAF colonel and nonresident senior fellow at the Center for Strategic and Budgetary Assessments, Dr. Haffa writes that the foundations of conventional deterrence are applicable to strategic competition today with modifications made to account for the current strategic landscape. He states that "most importantly, the greatest departure from Cold War formulations of conventional deterrence theory is the idea that it will be necessary to use force to create deterrence."[56] He supports this point by describing the potential deterrent effect of conventional forces being employed in the Iraq war.[57] Future development of multi-domain operations doctrine may consider the implications of conventional deterrence.

Dr. Mearsheimer's considerations for deterrence by denial are relevant today for multi-domain operations. He makes a point early on in his study that he is primarily focused on deterrence by denial, given that deterrence by punishment is mostly associated with nuclear weapons given their exceptionally destructive capabilities.[58] He defines conventional deterrence through a function of denial and not through a function of punishment.[59] Dr. Mearsheimer writes extensively on the use of PGMs as an enabling capability for conventional deterrence, and concludes that while PGMs are both an offensive and defensive capability, they primarily benefit the defensive actor through decreasing the odds of a successful adversary blitzkrieg.[60] By denying the adversary a potentially successful blitzkrieg strategy, PGMs support a deterrence by denial strategy. Future researchers looking to align MDO across the services may consider incorporating deterrence through denial by enabling the use of PGMs and like-weaponry. By enhancing deterrence through denial capabilities, this applicability supports aspects of integrated deterrence as defined by the 2022 NSS such as integration across domains and regions.[61]

---

[55] Robert Haffa, "The Future of Conventional Deterrence: Strategies for Great Power Competition" *Strategic Studies Quarterly* (Winter 2018). 100.

[56] Haffa, 111.

[57] Haffa, 111.

[58] Mearsheimer, *Conventional Deterrence*, 15.

[59] Mearsheimer, 15.

[60] Mearsheimer, 201.

[61] White House, *2022 National Security Strategy,* 22.

The other method of deterrence referenced – deterrence through punishment – is equally applicable. Dr. Karl Mueller of the RAND corporation writes that "among conventional deterrence strategies, punitive resistance is a straightforward threat."[62] It would be worthwhile for future researchers to consider contributing to deterrence by enhancing punitive resistance capabilities. This is directly supported by the 2022 NSS, which states that the U.S. must "convince potential adversaries that the costs of their hostile activities outweigh their benefits."[63]

Future researchers could draw two conclusions from these readings. First, researchers looking to apply deterrence theories must acknowledge the type or form of deterrence sought. Although multi-domain operations can contribute to both deterrence through punishment and denial, the way in which multi-domain operations is applied would differ. The doctrine required to use multi-domain operations to create a significant enough punishment to deter would be different from the doctrine used to create deterrence through denial, despite both being a form of multi-domain operations.

Second, any perceived threat being deterred should be analyzed in its geopolitical context. The relationship between PGMs and preventing conventional conflict has implications for a number of invasion-type scenarios U.S. forces may face. The geopolitical context of these scenarios strongly impacts how multi-domain operations function to prepare for this threat. How multi-domain operations contribute to punitive resistance to deter a conventional invasion of Taiwan would differ from an invasion of the Philippines or Japan and differ significantly from a Russian incursion into NATO territory. Simply put, future researchers and planners must clearly articulate both the form and function of multidomain operations if they wish to fully align this concept with integrated deterrence.

62 Karl Mueller, "The Continuing Relevance of Conventional Deterrence" in *Deterrence in the 21st Century—Insights from Theory and Practice* ed. by Frans Osinga and Tim Sweijs (The Hague, NL: T.M.C. Asser Press, 2020).

63 White House, *2022 National Security Strategy,* 22.

2. Classical Deterrence and Nuclear Deterrence Theory

Much of classical deterrence theory can be "traced to the early works of classical philosophers such as Thomas Hobbes, Cesare Beccaria, and Jeremy Bentham.[64] Dr. John Dilulio writes that the theory of deterrence developed from their writings has "three individual components: severity, certainty, and celerity."[65] In order for a deterrent to be effective, the punishment must be of an appropriate severity, certainty, and taken quickly in regard to the offense. Although these qualities were originally developed in terms of criminal punishment, such as described in Bentham's *Panopticon*, they lead directly into modern conceptions of nuclear deterrence.[66]

There is no authoritative definition of classical nuclear deterrence. However, Dr. Richard Snyder summarizes it as deterrence theory with "an emphasis on deductive logic and abstract analysis based largely on imaginary scenarios and nuclear deterrence."[67] Given it is potentially "the most influential school of thought in the American study of international relations," as Dr. Robert Jervis writes, it is worth analyzing.

Dr. Frank Zagare narrows down this definition by dividing classical deterrence theory into "two distinct, yet compatible, formulations: *structural* and *decision-theoretic*."[68] Dr. Zagare's distinction is useful given the broad number of theories which could fall under the term classical nuclear deterrence. This capstone focuses specifically on decision-theoretic deterrence, because the "interplay of outcomes, preferences, and (rational) choices in determining interstate conflict behavior" could assist future researchers in aligning multi-domain operations doctrine.

---

64 John Dilulio, *Deterrence Theory*. https://marisluste.files.wordpress.com/2010/11/deterrence-theory.pdf 234.

65 Dilulio, 235.

66 Jeremy Bentham, *The Panopticon Writings*, as presented by Matthieu Verry. Sorbonne Universite (2021).

67 Richard Snyder, "Book Review: Psychology and Deterrence by Robert Jervis, Richard Ned Lebow, and Nanice Gross Stein" *Political Psychology* 8, no. 2 (1987).

68 Frank Zagare, "Reconciling Rationality with Deterrence" *Journal of Theoretical Politics* 16, no. 2 (2004).

a. Decision-Theoretic Deterrence Theory

While Dr. Zagare defines structural deterrence theorists as "see [ing] the key to international stability in the distribution of power within the system in general, and among the great powers in particular," decision-theoretic deterrence theory focuses on rational actors[69] Dr. Zagare describes decision-theoretic deterrence theorists as those who "focus on the interplay of outcomes, preferences, and rational choices."[70] More simply, structural deterrence focuses on the playing field, while decision-theoretic models focus on individual players.

In fact, decision-theoretic deterrence can be summarized as deterrence modeled through "expected utility and game theory."[71] Dr. Zagare summarizes the decision-theoretic playing field as being the game of "chicken" and with individual players concluding that "war in the nuclear age is 'irrational.'"[72] This model assumes that all states are rational actors. Nuclear war is both the worst solution and the solution no rational actor would choose. To continue the metaphor, no player would willingly sacrifice the entire tournament for a single goal.

This theory is partially applicable to multi-domain operations. Unlike structural deterrence, parts of decision-theoretic deterrence are applicable to the multi-domain operations. The portion which is not applicable is that which is solely based upon nuclear warfare which results in total annihilation. The theory's emphasis on modeling game theory based on rational actors is applicable. This is because the multi-domain operations do not focus on the use of nuclear weapons but does discuss shaping perceptions to influence rational actors. For example, the most current version of U.S. Army FM 3-0 *Operations* frequently discusses shaping adversary perceptions through force posture and activities, but rarely discusses nuclear weapons outside of their operational and tactical

69 Frank Zagare, "Classical Deterrence Theory: A Critical Assessment" *International Interactions* 21, no. 4 (1996). 368.

70 Frank Zagare, "Reconciling Rationality With Deterrence A Re-Examination Of The Logical Foundations Of Deterrence Theory" *Journal of Theoretical Politics* 16, no. 2 (2004): 107–141.

71 Stephen Quackenbush, "Deterrence Theory: Where Do We Stand?" *Review of International Studies* 37, no. 2 (2011): 741–62. doi:10.1017/S0260210510000896.

72 Zagare.

implications.[73] The 2022 NSS states that the U.S. "cannot afford to rely solely on…nuclear deterrence." Therefore, it is worthwhile to create additional conventional deterrent capabilities in a nuclear world.[74]

The theory is most beneficial for informing multi-domain operations' inclusion of the competition continuum. By incorporating game theory, multi-domain operations can continually account for whether a rational actor should or should not continue to escalate within each phase of competition. For example, different aspects of multi-domain operations may have different effects on escalation depending on where those actors are located along the competition continuum. This is crucial given the 2022 NSS's emphasis on leveraging integrated deterrence to combat adversaries with "new strategies of threatening behavior below…the traditional threshold of conflict."[75]

3. Cyber Warfare and Cross-Domain Deterrence Theory

While classical deterrence theory substantially predates the cyber domain, there are commonalities between deterrence and cyber warfare that future researchers could consider when looking to align multi-domain operations. This section analyzes cyber deterrence in two formulations. The first formulation, classical cyber deterrence theory, is narrowly relevant multi-domain operations given its focus upon the deterrence of cyber operations through cyber operations alone. The second formulation, cross-domain deterrence theory, is more broadly applicable to multi-domain operations given their shared emphasis on the interaction of multiple domains.

a. Classical Cyber Deterrence Theory

Cyber deterrence by denial is both complex and dynamic. Unlike previous deterrence theories which focus on nuclear war, cyber deterrence must account for the possibility of a litany of state, non-state, and criminal actors with similar capabilities. Like previous deterrence theories, cyber deterrence by denial requires capability, credibility, and

[73] "FM 3-0: Operations," U.S. Army (October 2022).

[74] White House, *2022 National Security Strategy,* 22.

[75] White House, *22*.

communication between the actors. Advocates for cyber deterrence through denial propose that since the cyber domain is unique, deterrence actions should stay entirely within the domain.[76] Given the complex nature of cyberspace, other experts do not consider it a viable strategy.[77] They conclude that the low cost of cyber activity guarantees the failure of cyber deterrence by denial.[78] Future researchers could consider the value of cyber deterrence as part of a comprehensive multi-domain operations doctrine.[79]

The alternative to cyber deterrence by denial is deterrence by punishment. Similar to the international relations theory, cyber deterrence by punishment is based upon balancing threat of damage with the desirability of a certain action. Previous deterrence by punishment theories focused on the intense and novel destructive capability of nuclear weapons to perform this deterrence.[80] This power renders intimate details about potential targets – such as the material a building is constructed of or its distance in feet from a city-center – largely irrelevant. Cyber deterrence by punishment does not have this luxury, and does require an intimate understanding of the target.[81] Cyber capabilities are extremely dependent upon their target, and are often times only useful against one target in particular.[82] In turn, cyber deterrence by punishment may be less achievable than nuclear deterrence by punishment.[83]

---

[76] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?." *Journal of Strategic Security* 7, no. 1 (2013): 54–67. DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5

[77] Iasiello, 54–67.

[78] Iasiello, 54–67.

[79] Martin Libicki, *Conquest in Cyberspace* (Cambridge: Cambridge University Press, 2007).

[80] Bernard Brodie, ed., The Absolute Weapon (New York: Harcourt Brace, 1946).

[81] Thomas Rid and Peter McBurney, "Cyber-Weapons" *The RUSI Journal* (February/March 2012). 12.

[82] Thomas Rid and Peter McBurney, "Cyber-Weapons" *The RUSI Journal* (February/March 2012). 12.

[83] Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?." 54–67.

b. Cyber and Cross-Domain Deterrence

Cross-domain deterrence can include cyber deterrence as a cross-cutting mechanism.[84] Cyber and non-cyber actions may not be perfectly analogous, but multi-domain operations can allow reciprocal if not identical effects. The actions do not necessarily need to be kinetic. The costs imposed by cross-domain deterrence, whether for denial or punishment, could include but are not limited to economic sanctions, loss of credibility, or legal enforcements.[85] Cross-domain deterrence is largely considered to make up for the shortfalls of cyber deterrence.[86] Despite this, cross-domain deterrence does not make up for all of the shortfalls of cyber deterrence. Similar to cyber deterrence, cross-domain deterrence introduces a larger number of actors to consider.[87] In addition to cyber deterrence, it also increases the number of actions each actor can take.[88] Cross-domain deterrence is more theoretically sound but less objectively measurable.[89]

Readings on cross-domain deterrence are potentially useful for aligning U.S. Army and USAF multi-domain operations. It is appropriately scoped and includes consideration of actions taken within a state. It is appropriate for the competition continuum as it does not solely focus on deterrence through the use of a unique capability but instead multiple and varying capabilities. Perhaps most importantly, cross-domain deterrence focuses on the interplay of actions across domains in a way previous deterrence theories do not.[90] Given how new cross-domain deterrence is, readings should be continually evaluated for their contribution to multi-domain operations.

---

[84] Jon Lindsay and Erik Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York, NY: Oxford University Press, 2019).

[85] King Mallory, "New Challenges in Cross-Domain Deterrence," Perspective. (RAND: Santa Monica, CA: 2018).

[86] Jon Lindsay and Erik Gartzke, *Cross-Domain Deterrence.*

[87] King Mallory, "New Challenges in Cross-Domain Deterrence," Perspective. (RAND: Santa Monica, CA: 2018). 2.

[88] King Mallory, "New Challenges in Cross-Domain Deterrence," 7.

[89] Jon Lindsay and Erik Gartzke, *Cross-Domain Deterrence.*

[90] Lindsay and Gartzke, *Cross-Domain Deterrence.*

C. CONCLUSION

As Dr. John Mearsheimer stated in *Conventional Deterrence*, "a potential attacker's fear of the consequences of military action lies at the heart of deterrence."[91] Since then, technological developments have created new domains of warfare, and new avenues for states to inflict damage against one another. As this chapter demonstrates, a strategy of integrated deterrence must consider actions across all domains based on a nuanced understanding of the actors. Multi-domain operations doctrines should then incorporate these theories in order to support the overall strategy.

Conventional deterrence builds ideas such as strategies of limited aims or attrition and how best to deter them. Nuclear deterrence tackles strategic interaction through the use of the game "Chicken" and modeling actor behavior. The former provides great insight into how the proliferation of technology, among other things, can change state decision making, while the latter focuses on how mathematically modeling potential state actions can yield insightful results. Cross-domain deterrence informs how deterrence effects can be used by appropriately matching operations across domains based on adversary perceptions. While all of the deterrence theories are worth reviewing, cross-domain deterrence has the most applicability for suggesting doctrinal changes which better align USAF and U.S. Army concepts of multi-domain operations.

[91] Mearsheimer, *Conventional Deterrence*, Chapter 2.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MULTI-DOMAIN OPERATIONS READINGS

As a general statement, the concept of multi-domain operations is not new – commanders have synchronized operations across domains, such as land and maritime, for centuries. What are new are the service concepts which describe how they plan to evolve multi-domain operations. This chapter analyzes multi-domain operations in order to better understand where and how U.S. Army and USAF doctrines might be aligned. It begins by reviewing discussions produced on multi-domain operations by a variety of practitioners and academic scholars. Next, it breaks down and analyzes multi-domain operations as presented by the U.S. Army, which focuses on the key tenet of long-range fires, and the USAF, which focuses on key tenet of command and control. Finally, it cross-references the key tenets of the various multi-domain operations doctrines with requirements stated by the 2022 NSS to demonstrate the interaction between multi-domain operations and integrated deterrence.

A. DISCUSSIONS ON MULTI-DOMAIN OPERATIONS

Lt. Col. Kelly McCoy writes in "The Road to Multi-Domain Battle: An Origin Story" on the history of U.S. Army multi-domain operations. Lt. Col. McCoy provides context to multi-domain operations' historical journey by describing both joint and other-service doctrines concurrently developing. Lt. Col. McCoy's analysis is extremely helpful for understanding the many individual events which led to the creation of Army multi-domain operations.[92]

In "Accelerating Multi-Domain Operations," General Stephen Townsend makes the case for U.S. Army multi-domain operations as the commander, U.S. Army Training and Doctrine Command. General Townsend's writings provide insight into the applied and non-theoretical side of the development of multi-domain operations. The author provides evidence of both the U.S. Army and USAF having separate but extremely similar

[92] Kelly McCoy, "The Road to Multi-Domain Battle: An Origin Story." Modern War Institute at West Point. October 2017. https://mwi.usma.edu/road-multi-domain-battle-origin-story/

conceptions of multi-domain operations, which is a crucial part of this capstone' analysis.[93]

Maj. Grant Smith writes in "Multi-Domain Operations: Everyone's Doing It, Just Not Together" on the shortcomings of multi-domain operations as a joint activity. He acknowledges where each of the services are with regards to multi-domain operations and how they view performing further research. Although his conclusion is primarily based on education and training for future officers, and outside the scope of this capstone, his writing informs the history of multi-domain operations.[94]

In "Multi-Domain Operations: Bridging the Gaps for Dominance" Maj. Kimber Nettis writes on the intersection of topics such as "AirLand Battle," "Multi-Domain Operations," and "Hybrid Warfare."[95] To combine these, she creates a multi-domain operations framework which accounts for multiple warfighting domains and cross-cutting sectors. The intention of her framework is to improve analysis performed on the challenges of multi-domain operations. Maj. Nettis describes the 88th Air Base Wing's attempts to institutionalize a wing-level multi-domain command and control structure as one manner of implementing the framework. Her research represents some of the latest discussion thought on multi-domain operations.

"The Application and Employment of Special Forces to Effectively Operate in the Multi-Domain Operations Environment of Large-Scale Combat Operations" by Artur Dominiak and John Bassette analyze the role of U.S. Army Special Forces in supporting conventional forces while adapting to multi-domain operations. They write that the "SF force structure currently lacks some of the capabilities to effectively operate and thrive on

93 Stephen Townsend, "Accelerating Multi-Domain Operations." *Military Review* (September-October 2018)..

94 Grant Smith, "Multi-Domain Operations: Everyone's Doing It, Just Not Together." Other The Horizon: Multi-Domain Operations and Strategy. June 2019. https://othjournal.com/2019/06/24/multi-domain-operations-everyones-doing-it-just-not-together/

95 Kimber Nettis, "Multi-Domain Operations: Bridging the Gaps for Dominance," *Wild Blue Yonder*. (Maxwell AFB: Air University Press, 2020).

the modern battlefield.[96] The authors recommend that "SF units should reconsider their capabilities when it comes to penetrating and disabling the anti-access area denial (A2/AD) bubbles" and "should also consider the tools required to destroy or disable A2/AD."[97] Among other recommendations, they conclude that "at a minimum, SF needs to add an EW/cyber MOS to its team structure if it is to remain relevant."[98]

This source is the work of two U.S. Army Special Forces officers' writing on how to integrate Special Forces into multi-domain operations based on both their research and individual experiences. The topic aligns strongly with this capstone, although it focuses on tactical level recommendations and only on Special Forces and not the Joint Force. The authors' focus on the A2/AD problem-set serves as evidence of U.S. Army multi-domain operations' key tenets.

"Multiple Dilemmas for the Joint Force: Joint All-Domain Command and Control" by Dr. Miranda Priebe et al. "summarizes research results that identified potential impediments to multi-domain operations in the current operational C2 construct for joint operations."[99] The authors conducted over 150 interviews and developed four alternative "joint all-domain C2 (JADC2) constructs."[100] The authors conclude that two priorities for a "high-end" fight must include "global integration for transregional conflict" and "distributed control for a communications-contested environment."[101] They identify that both multi-domain operations and JADC2 have multiple proposed evolutions developing in parallel, creating potential confusion. The authors recommend doctrine writers clarify the role of multi-domain operations in order to clarify the supporting role of command and control.

---

[96] Artur Dominiak and John Bassette, "The Application And Employment Of Special Forces To Effectively Operate In The Multi-Domain Operations Environment Of Large-Scale Combat Operations." Capstone, *Naval Postgraduate School* (December 2021).

[97] Dominiak and Bassette, v.

[98] Dominiak and Bassette, 61.

[99] Miranda Priebe et al.,Multiple Dilemmas for the Joint Force: Joint All-Domain Command and Control. Santa Monica, CA: RAND Corporation, 2020.

[100] Priebe et al., 1.

[101] Priebe et al., 2.

Dr. Priebe et al. take care in this research summary to differentiate between multi-domain operations and command and control. Of particular note is their inclusion of considerations for planning offensive cyberspace operations, which is not present in most material on multi-domain operations. Still, it is apparent that this RAND study focuses on the Air Force conception of multi-domain operations including an emphasis on command and control. Their various models of command and control are beneficial for recognizing the limitations of multi-domain operations as planned by a single service. This research demonstrates a shortcoming within the Joint Force's ability to meet the technical requirements of multi-domain command and control.

"Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran, and North Korea" by James Black et al. is a RAND Europe product that "aims to review existing literature and perspectives on whether potential UK adversaries … are developing similar or equivalent concepts of [multi-domain operations]."[102] Although the majority of this research focuses on fitting adversary operations into Western conceptions of multi-domain operations, the main value for this capstone comes from its analysis of Western multi-domain operations. The authors write on multi-domain operations primarily from the perspective of the United Kingdom and NATO, which is similar, but not identical, to both U.S. Army and USAF multi-domain operations.

Most effective from this document are its attempts to differentiate between the growing and often-confusing lexicon surrounding multi-domain operations.[103] The authors also tackle common questions such as "How is 'multi-domain' different from and related to 'joint'" and "How is 'multi-domain' different from and related to 'sub-threshold' or 'grey zone' operations."[104] The authors identify the "recent flurry of theoretical and empirical work…examining cross-domain aspects of strategy."[105] While they do not

[102] James Black et al., Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea. Santa Monica, CA: RAND Corporation, 2022.

[103] Black, "Multi-Domain Integration in Defence," 9.

[104] Black, 9–11.

[105] Black, 10.

necessarily draw any conclusions of their own with regards to this summary, they recognize the term as linking multi-domain operations to deterrence thinking.

In "Multi-Domain Operations and Information Warfare in the European Theater" by Maj. Jennifer Purser, the author examines Operation Dragoon Ride 2015 as a case study for the interaction of information warfare and multi-domain operations.[106] The author writes that this case study provided lessons learned on how to integrate information operations with shaping activities while facing an "[information warfare]-savvy" adversary. She concludes that U.S. Army units must have strategies for managing their information and public affairs presence in order to effectively integrate within multi-domain operations.

B. CONCEPTS OF MULTI-DOMAIN OPERATIONS

There is not one accepted definition of multi-domain operations nor is there an agreed upon concept at the joint level. Instead, the term generically refers to a number of different ideas. The U.S. Army and USAF have developed the two most well-known concepts to-date. Before this chapter outlines how multi-domain operations meet integrated deterrence's requirements, it first must make clear what version of multi-domain operations it is referring to. This section distills key tenets from both U.S. Army And USAF multi-domain operations. These key tenets provide a reference point later on for understanding where the service doctrines could potentially better align.

1. U.S. Army Multi-Domain Operations and Long-Range Fires

By reviewing the recent evolution of Army multi-domain operations, its key tenet which has consistently been a part of the concept is described. The review begins with then-Deputy Secretary of Defense Bob Work's speech at the Army War College and ends with the current version of joint-all domain operations. A distinction is made between core tenets, which are organic to the Army multi-domain operations as described in Army

106 Jennifer Purser, "Multi-Domain Operations and Information Warfare in the European Theater," *Military Review* (November-December 2020).

doctrine, and the key tenet, which this chapter derives through analysis of multiple writings.

According to Lt. Col. Kelly McCoy, Strategy Chair at the Naval Postgraduate School's National Security Affairs Department, "the origins of Multi-Domain Battle can be traced back to April 8, 2015 at the U.S. Army War College, where then Deputy Secretary of Defense Bob Work charged the U.S. Army to get after AirLand Battle 2.0."[107] During this speech, Secretary Work emphasized themes such as "enemies which have lots of guided rockets… and are using informationalized warfare to completely disrupt our heavily netted force."[108] Deputy Secretary Work was describing the early setting of two key problem sets: first, how to defeat adversary long range-fires. Second, how to defeat an adversary's highly interconnected information system while maintaining one's own information system. It is impossible to know without asking him, but by "informationalized" warfare it is likely Deputy Secretary Work was referring to what RAND now describes as the "strategic guidelines [which] direct the PLA to win 'Informatized Local Wars."[109] Both of these requirements would go on to become key tenets in the Army multi-domain operations in the form of a focus on long-range fires and leveraging the information domain.

In 2015, Deputy Secretary Work originally described AirLand Battle 2.0 as focused on conflict. As it evolved in the next year, its scope would increase to include cooperation and competition under the new title "Multi-Domain Battle." Lt. Col. McCoy writes that Multi-Domain Battle Concept Version 1.0 "examines three key ideas: (1) Competition and the Conflict Continuum; (2) Compression, Convergence, and Expansion of the Battlefield;

[107] Kelly McCoy, "The Road to Multi-Domain Battle: An Origin Story." Modern War Institute at West Point. October 2017. https://mwi.usma.edu/road-multi-domain-battle-origin-story/

[108] Bob Work, "Army War College Strategy Conference" (2015), U.S. Department of Defense, https://www.defense.gov/News/Speeches/Speech/Article/606661/army-war-college-strategy-conference/

[109] Edmund Burke, Kristen Gunness, Cortez Cooper, and Mark Cozad, "People's Liberation Army Operational Concepts" (2020), RAND Corporation. https://www.rand.org/pubs/research_reports/RRA394-1.html

and (3) the Future Force Components."[110] He demonstrates that in order "to compete (and prevail), you must directly link your capability of waging all-out war with what you do in competition."[111] While AirLand Battle 2.0 was focused primarily on conflict, multi-domain operations opened the aperture to the full range of competition. This is significant due to integrated deterrence requiring the Department of Defense to operate in all phases of strategic competition.

Two years later, critics criticized Multi-Domain Battle as being both too vague and non-innovative.[112] Continually expanding scopes and responsibilities rendered the core tenets unclear. In response to this and other criticism, on May 23, 2018, General Townsend, then the commander of U.S. Army Training and Doctrine Command, announced at the Land Forces Pacific Symposium that Multi-Domain battle would be transitioning to multi-domain operations. In that position, he was the final authority on the Army's "Multi-Domain Battle concept." He elaborated on his speech in Army University Press: "Over the last eighteen months that Multi-Domain Battle has been out there for debate, there have been four consistent critiques."[113] These are that critics perceive Multi-Domain Battle as "old wine in a new bottle," that it is an Army-only concept, that it is too tactical and does not leave enough room for transforming culture, and that it focuses on battle, and not on competition.[114] This was important in that General Townsend recognized that Multi-Domain Battle as a term that was becoming unclear.

General Townsend would further elaborate the core tenets of multi-domain operations in a 2018 Training and Doctrine Command Pamphlet. Titled 525–3-1 *The U.S. Army in Multi-Domain Operations 2028,* he describes multi-domain operations as "the

---

110 Kelly McCoy, "Competition, Conflict, and Mental Models of War: What you Need to Know About Multi-Domain Battle." Modern War Institute at West Point. January 2018. https://mwi.usma.edu/competition-conflict-mental-models-war-need-know-multi-domain-battle/

111 McCoy, "Competition, Conflict, and Mental Models of War."

112 Richard Sinnreich, "Multi-domain battle: Old Wine In A New Bottle?" *Army*, 67(2), 13–14. (2017).

113 Stephen Townsend, "Accelerating Multi-Domain Operations." *Military Review*, September-October 2018. (Army University Press, 2018).

114 Townsend.

rapid and continuous integration of all domains of warfare" to "deter and prevail as we compete short of armed conflict" by solving the problem of "layered standoff."[115] According to Townsend, multi-domain operations are composed of "three core tenets" which the U.S. Army must focus on: calibrated force posture, multi-domain formations, and convergence.[116] It is not clear whether or not the 2018 pamphlet settled any of the prior criticisms. At one-hundred pages long, the pamphlet introduces a significant amount of information without making entirely clear the focus of multi-domain operations.

Within this document is evidence that multi-domain operations focus on long-range fires and leveraging the information domain had persisted from AirLand Battle 2.0. Within the first figure, the authors write that the main challenge for multi-domain operations is "Russian and Chinese Anti-Access and Area Denial Systems Create Multiple Layers of Stand-Off."[117] It emphasizes the need for "forward presence forces, national-level capabilities, independent maneuver, and cross-domain synergy."[118] While neither quote is a direct translation of AirLand Battle 2.0's requirements, they signify adherence to the original core tenets of long-range fires and leveraging the information domain.

U.S. Army multi-domain exercises that same year provide more evidence to this point. In 2018, the Army's Multi-Domain Task Force pilot effort launched, focusing on "long-range fires" while integrating "intelligence, cyber, electronic warfare, and space" at the headquarters level.[119] Originally tested in the USINDOPACOM area of responsibility, the Multi-Domain Task Force was "designed to counter an adversary's anti-access/area denial…capability" by "employing organic, joint, and multi-national capabilities in all domains: air, sea, land, space, and cyber, as well as information operations and the human

[115] U.S. Army Training and Doctrine Command, "TRADOC Pamphlet 525-3-1 The U.S. Army in Multi-Domain Operations 2028," (Washington, DC: U.S. Army Training and Doctrine Command, 2018), Preface.

[116] U.S. Army Training and Doctrine Command, Preface.

[117] U.S. Army Training and Doctrine Command, Figure 1.

[118] U.S. Army Training and Doctrine Command, Figure 1.

[119] Sean Kimmons, "Second Phase of Multi-Domain Task Force Pilot headed to Europe," United States Army. October 2018. https://www.army.mil/article/212342/second_phase_of_multi_domain_task_force_pilot_headed_to_europe

domain."[120] As Charles McEnany, a National Security Analyst at the Association of the United States Army, states, "MDTFs seek to gain and maintain contact with the adversary in the competition phase, to contribute to de-escalation back to competition during a crisis and, should conflict occur, to help disrupt enemy A2/AD to enable Joint Force maneuver."[121] As can be seen both in a nuanced reading of the Army's multi-domain doctrine as well as their multi-domain exercises, the key tenets remain long-range fires and leveraging the information domain. These tenets will be integral to an understanding of joint multi-domain operations.

2. The USAF and Multi-Domain Command and Control

Similar to the U.S. Army, The USAF developed its own vision for the term "multi-domain operations." Also similar to the Army, the Air Force's vision for multi-domain operations, and its key tenet, has become less clear overtime. As the vision has developed its scope and purpose have expanded. This section reviews the recent history of Air Force multi-domain operations in order to understand its key tenet for later application. An examination of multiple Air Force multi-domain initiatives will demonstrate that the key, unifying tenet is command and control. Furthermore, there exists an emphasis on the role technology plays in multi-domain operations.

The Air Force's multi-domain inception began with the publication of *Concept for Future Air Force Operations 2035* in September 2015 – just five months after Deputy Secretary Work's speech on AirLand Battle 2.0.[122] The document defines its central idea as agility, or "the ability to act appropriately within a changing context" with the purpose of "[placing] an adversary on the 'horns of multiple dilemmas.'"[123] It defines "Integrated Multi-Domain operations" as encompassing "interoperability among air, space, and cyberspace capabilities so that the combined effect is greater than the sum of the

120 Kimmons.

121 "Multi-Domain Task Forces: A Glimpse at the Army of 2035." Association of the United States Army, March 2022. https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035.

122 "Air Force Future Operating Concept: A View of the Air Force in 2035." Internal report (September 2015). https://www.af.mil/Portals/1/images/airpower/AFFOC.pdf

123 "Air Force in 2035," 7.

contributed parts without being limited by rigid interdependence."[124] Although "integrated multi-domain operations" was listed as a specific concept, the document specifically defines "multi-domain command and control" as a future Air Force core capability.[125] These quotes emphasize the two most important tenets of Air Force multi-domain operations: presenting adversaries with multiple dilemmas and creating interoperability between domains.

The Air Force's *Air Superiority 2030 Flight Plan* was the next strategic document which defined the Air Force multi-domain operations. Released in 2016, the plan documented multi-domain operations as one part of many future investments needed "as part of the Anti-Access/Area-Denial (A2/AD) strategy in highly contested environments."[126] This emphasis on the problem is important for understanding the Air Force multi-domain operations, as it represents a synergy with the Army's then Multi-Domain Battle concept. While both ideas were solving similar problems, they were presenting alternative solutions based on their own service's perception of the problem. It becomes increasingly important to delineate between what a service is tracking internally as a key tenet, and what it is accepting as a function of parallel and synergistic efforts.

Future Air Force Operations 2035 also featured an early indication of the required 'jointness' of multi-domain operations. It notes that "it is only when operations in these domains are effectively integrated with those in the land and maritime domains that the joint team will be able to reach its true potential."[127] It may seem obvious that multi-domain operations would be joint. However, that does not appear to have been the case at all times. Maj. Grant Smith, then a student of the Air Force's Multi-Domain Operational Strategist program, writes in 2019 that "the Air Force [places] its focus on Multi-Domain

124 "Air Force in 2035," 8.

125 "Air Force in 2035," 14.

126 Enterprise Capability Collaboration Team, "Air Superiority 2030 Flight Plan." United States Air Force, May 2016.

127 "Air Force in 2035," 9.

Command and Control…within the domains of air, space, and cyberspace."[128] Unlike the Army's vision of multi-domain operations which focuses on achieving objectives with effective long-range fires, the Air Force's vision of multi-domain operations focuses instead on achieving effects through enhanced command and control.[129]

The Air Force's commitment to command and control continued outside of these published documents. The concept document in 2015 describes a "multi-domain operations center" as a replacement for the theater-level air operations center.[130] In 2018, the Air Force began running "Doolittle Series" war games at the LeMay Doctrine Center in Montgomery, Alabama.[131] Of the wargames, Maj. Smith writes:

> Participants were primarily from within the Air Force and separated into teams to develop the best C2 structure to use in conflict with a peer adversary. However, the exercise's primary agenda seemed to be narrowly focused on one thing: the transformation of the Air Operations Center (AOC) into a Multi-Domain Operations Center (MDOC). Shifting focus from how the Air Force currently conducts operations to preparing for tomorrow's fight will take more than just a title change of the Air Force's primary command and control facility. The fact that joint partners were largely excluded from this exercise is rather disappointing when considering the multi-domain and C2 capabilities the other services can offer.[132]

Despite documentation which state adherence to joint integration and adversary anti-access/area denial, these exercises provided additional proof that the Air Force's concept of multi-domain operations focused on enhancing command and control.

Another feature of the Air Force's approach to multi-domain operations is its establishment of several multi-domain-themed specialties. As the Doolittle Series

---

[128] Grant Smith, "Multi-Domain Operations: Everyone's Doing It, Just Not Together," Other The Horizon: Multi-Domain Operations and Strategy. June 2019. https://othjournal.com/2019/06/24/multi-domain-operations-everyones-doing-it-just-not-together/

[129] "Air Force Future Operations Concept: A View of the Air Force in 2035," United States Air Force, September 2015.

[130] "Air Force Future Operations Concept: A View of the Air Force in 2035," United States Air Force, September 2015.

[131] "Doolittle Series 18: Multi-Domain Operations," (Maxwell AFB: Air University Press, 2019).

[132] Smith, "Everyone's Doing It,"

concluded, "There is a need for highly trained and operationally experienced personnel in Command and Control."[133] Following this, Chief of Staff of the Air Force General David Goldfein established the 13O Air Force Specialty Code – Multi-Domain Warfare Officers—through the "Multi-Domain Command and Control (MDC2) Implementation Plan.[134] In addition to creating the new officer specialty, the implementation plan established "an Architecture Office led by a Multi Domain Command and Control lead architect" for the purpose of integrating advanced technology and the creation of "an Air Force data strategy that details the Air Force's adoption of modern data management techniques and a family of standards for data."[135] Through both of these developments, the Air Force continued emphasizing the role of command and control in multi-domain operations.

The Air Force's approach to multi-domain education provides more evidence of command and control as a key tenet. In 2020 Maj. Kimber Nettis, then deputy director for the Cyber Professional Continuing Education Program at the School of Strategic Force Studies, provides a deeper analysis of Air Force multi-domain operations concepts in the Air University journal *Wild Blue Yonder*. She writes that "situational awareness capabilities are not designed to provide an integrated understanding of the battlespace that spans all domains, and command and control constructs do not provide the necessary agility to synchronize effects."[136] To this end, she describes the Air Force's multi-domain command and control initiative as a requirement to support multi-domain operations for the Joint Force.[137]

Although as of 2022, the USAF has begun shuttering the 13O career field, this has not stunted the Air Force's multi-domain operations progress. As the Air Force has combined its technological and educational initiatives into the Joint All-Domain

133 "Doolittle Series 18," 2.

134 Heather Wilson, David Goldfein, and Kaleth Wright, "Multi-Domain Command and Control (MDC2) Implementation Plan," June 2018.

135 Wilson, Goldfein, and Wright, "Implementation Plan," 3.

136 Nettis, "Bridging the Gaps."

137 Nettis, "Bridging the Gaps."

Operations framework, the specific career field shut down. As now Chief of Staff of the Air Force General CQ Brown said, "To continue outpacing near-peer adversaries, we must reinforce all Air Force members' multi-domain expertise."[138]

Sometimes lexicons fall into and out of favor so quickly that terminology becomes overlapping and conflicting. As of March 2022, the Joint Staff defined their Multi Domain Operation command and control program as Joint All-Domain command and control. Despite the name change, the joint concept led by the Air Force remains similar to the Air Force's focus on multi-domain command and control. The *Joint All-Domain Operations Command and Control Strategy Implementation Plan* provides additional evidence in its stated purpose:

> JADC2 provides a coherent approach for shaping future Joint Force C2 capabilities and is intended to produce the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed of relevance.[139]

The evolution of terms has assisted in bringing U.S. Army and USAF multi-domain operations closer together. In September 2020 both service chiefs signed a memorandum which agreed to "establish Combined Joint All-Domain Command and Control at the most 'basic levels' by defining mutual standards for data sharing and service interfacing in an agreement that will run until the end of fiscal year 2022."[140] In this case, the word "combined" was added to the joint concept to indicate integration with foreign partner nations. Specifically, this agreement dictated that the Air Force headquarters staff lead integration between the Army's Project Convergence, which is the technological component of their multi-domain operations, and the Air Force's Air Battle Management System, which is a core technical component of their future command and control structure.

---

[138] Secretary of the Air Force Public Affairs, "Air Force to Phase Out 13O Career Field, Strengthen All Airmen Joint Capabilities," Press release, February 2022. https://www.af.mil/News/Article-Display/Article/2938234/air-force-to-phase-out-13o-career-field-strengthen-all-airmen-joint-capabilities/

[139] "Summary of the Joint All-Domain Command and Control (JADC2) Strategy," Joint Staff. March 2022. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

[140] Joe Lacdan, "Army, Air Force Form Partnership, Lay Foundation for CJADC2 Interoperability," Army News Service. October 2020. https://www.af.mil/News/Article-Display/Article/2369626/army-air-force-form-partnership-lay-foundation-for-cjadc2-interoperability/

Despite the additional names which exist, for the purposes of consistency this capstone will remain focused on the term "multi-domain operations" to reduce confusion.

C. THE KEY TENETS OF MULTI-DOMAIN OPERATIONS

As reviewed in earlier chapters, the U.S. 2022 NSS lays out five requirements for integrated deterrence. These are integration across domains, regions, the spectrum of conflict, the U.S. government, and with allies and partners.[141] Of these, the key tenets of multi-domain operations explicitly match four of them. The one requirement not met—integration with the U.S. government—is comprehensive and an overarching problem for multi-domain operations to respond to, and so will be outside the scope of this capstone. For the remaining four requirements, this section matches each requirement of integrated deterrence to one or more key tenets of multi-domain operations. Given the broad scope of multi-domain operations and the key tenets themselves, it is arguable that each key tenet supports all requirements of integrated deterrence. This section only matches key tenets to requirements they primarily support.

1. Long-Range Fires and Command and Control

The key multi-domain operations tenet of long-range fires supports the integrated deterrence requirements of integration across domains and regions. The Congressional Research Service summary of the Army's Multi-Domain Task Force succinctly explains why:

> What Is a Multi-Domain Task Force? In the *Army's Chief of Staff Paper #1: Army Multi-Domain Transformation Ready to Win in Competition and Conflict* dated March 16, 2021 the Army describes the Multi-Domain Task Force (MDTF) as "theater-level maneuver elements designed to synchronize precision effects and precision fires in all domains against adversary anti-access/ area denial (A2/AD) networks in all domains…[142]

The paper elaborates that the multi-domain task force will have a "mid-range capability battery" and "long-range hypersonic battery" in addition to a [High Mobility

[141] White House, National Security Strategy, 22.

[142] "The Army's Multi-Domain Task Force (MDTF)," Congressional Research Service (May 2022). https://sgp.fas.org/crs/natsec/IF11797.pdf

Artillery Rocket System] battery for providing strike capabilities across multiple regions. An "All-Domain Operations Center" which will "enable 24/7 monitoring of adversary activities in all domains" will support these batteries.[143] These capabilities directly support the integrated deterrence requirements for integration across regions and domains.

Including long-range fires within a theater will pose several questions. These include geographical and legal questions regarding suitability and permissions. The U.S. Army, USAF, and United States Marine Corps can effectively today provide long-range fires. The U.S. Navy is currently developing more mature long-range fires technology, such as hypersonic missiles.[144] Future planning considerations will have to evaluate which of these technologies or services is best poised to support multi-domain operations' long-range fires, even if the author primarily derives the long-range fires key tenet from U.S. Army multi-domain operations.

The key multi-domain operations tenet derived from the Air Force—multi-domain command and control—directly supports all integrated deterrence requirements. As a joint function, the Joint Force recognizes command and control as inherent to any military operation.[145] By that logic, multi-domain command and control inherently supports any military operation to include those which support the Department of Defense's role in multi-domain operations. Multi-domain command and control achieves this through creating compatible technological, procedural, and legal standards for involved operations.

There exist criticisms of whether or not multi-domain command and control is feasible and, if so, how the Joint Force would implement it. Mark Seip, a retired Navy captain and adjunct assistant professor at Georgetown University's Edmund A. Walsh School of Foreign Service Center for Security Studies, articulates concerns about the key tenet's technical backbone. "The premise of [multi-domain command and control] — the

143 "The Army's Multi-Domain Task Force (MDTF)," Congressional Research Service (May 2022). https://sgp.fas.org/crs/natsec/IF11797.pdf

144 Caitlin Kenney, "The Naval Brief: Long-range fires experimentation; Hypersonic development tests; Red Hill defueling; and more..," DefenseOne (October 2022). https://www.defenseone.com/threats/2022/10/the-naval-brief-october-27-2022/379010/

145 "Joint Publication 3-0, Joint Operations Incorporating Change 1," Joint Staff (October 2018).

capability to link the various kill chain nodes seamlessly throughout the battlespace — reads really well" he writes.[146] He continues that "[multi-domain command and control's] goal of a fully immersed, across-the-battlespace network — while ambitious and well-meaning — is simply unrealistic."[147] His primary criticism is that multi-domain command and control relies too heavily on centralized information systems which adversaries will easily disrupt during conflict. Professor Seip's concern is valid and creates a new requirement for the implementation of multi-domain command and control. Such a system must be able to resist or, at a minimum flex, to adversary attempts to disrupt or destroy it. The more complicated a system is, the more difficult it is to build it in a flexible and resilient manner.

2. Information—Influence and Warfare

The advent of the information domain is related to the last two multi-domain key tenets—influence operations and non-kinetic fires. The first tenet is the ability to influence populations, and the second tenet is the ability to integrate non-kinetic fires. Taken together, both meet all of the requirements of integrated deterrence, but leverage the informational domain in distinct manners from one another.

The tenet of influence operations meets all four integrated deterrence requirements, to include integration across the spectrum of conflict and integration with allies and partners. This makes this tenet the most broadly supporting tenet of multi-domain operations, and the most efficient in terms of investment. This is because operations across all domains, both near and far, influence human beings by physical or virtual means.[148]

[146] Mark Seip, "Bad Idea: All Sensors, All Shooters, All the Time – a Joint All-Domain Command and Control System That Prioritizes Centralization" Defense360 (December 2020). https://defense360.csis.org/bad-idea-all-sensors-all-shooters-all-the-time-a-joint-all-domain-command-and-control-system-that-prioritizes-centralization/

[147] Mark Seip, "Bad Idea,"

[148] Robert Cordray and Marc Romanych, "Mapping the Information Environment," *IO Sphere* (Summer 2005).

Influencing populations inherently requires working with allies and partners to understand their particular needs and capabilities.[149]

The second tenet is leveraging the information domain to integrate non-kinetic fires. Although the term "non-kinetic fires" has many definitions depending on the audience, for the purposes of this capstone, the term "non-kinetic fires" refers to offensive actions taken in the cyber domain or through the electromagnetic spectrum, regardless of the domain they originate from. This tenet directly supports the integrated deterrence requirements of integration across domains, regions, and the spectrum of competition. As Franz-Stefan Gady and Alexander Stronell at the NATO Cooperative Cyber Defence Centre of Excellence write, "Synchronized kinetic and cyber operations across domains that present 'multiple dilemmas' are a fundamental tenet of multi-domain operations."[150] The Army's multi-domain task force concept's intelligence, information, cyber, electronic warfare, and space battalion demonstrates these ideas.[151] This tenet supports both other key tenets of multi-domain operations and requirements of integrated deterrence itself.

D. CONCLUSION

Despite the services not having a unified vision for multi-domain operations, there are key tenets from each which, when combined, meet the requirements for integrated deterrence as articulated by the 2022 NSS. Despite there being no agreed-upon concept of multi-domain operations at the joint level and service-level multi-domain operations have become unclear due to increasing scope, analyzing the services' recent multi-domain operations histories made affirming these key tenets possible. These key tenets are long-range fires, command and control, influencing populations, and integration non-kinetic fires. When taken together, the combination of these tenets supports the four applicable integrated deterrence requirements of integration across domains, regions, the spectrum of

[149] Lori Reynolds and Thomas Rid, "Competing for Influence: Operations in the Information Environment," Podcast. Modern Warfare Institute (January 2021).

[150] Franz-Stefan Gady and Alexander Stronell, "Cyber Capabilities and MultiDomain Operations in Future High-Intensity Warfare in 2030," *Cooperative Cyber Defence Centre of Excellence* (2020). 152.

[151] "The Army's Multi-Domain Task Force (MDTF)," Congressional Research Service (May 2022). https://sgp.fas.org/crs/natsec/IF11797.pdf

competition, and allies and partnerships. This understanding of multi-domain operations can be used by future research efforts which seek to align U.S. Army and USAF multi-domain operations concepts and their accompanying doctrines.

IV. OTHER RELATED RESEARCH

The author of this capstone participated in multiple trips in support of this research. These trips included briefings and small group discussions where information was exchanged regarding the participating units and research being conducted. In many cases, the trips were able to directly contribute to ongoing unit requirements. Relevant information is provided for the most significant trips and meetings conducted during this research. No interviews were conducted in support of this research.[152]

From 18 September to 25 September 2021, and 6 November to 13 November 2021, the author participated in the NATO Energy Security Center of Excellence exercise CORE 21 in Vilnius, Lithuania and Kyiv, Ukraine. The author's participation was as a subject matter expert in multi-domain operations and strategic communications/information operations. Exercise participants included representatives from the Swedish, Estonia, Latvian, Lithuanian, and Ukrainian governments. The author was able to contribute significantly to partner force ability to leverage multi-domain and information environment operations per the stated goals of the NATO exercise. Information developed during these exercises informed the author's understanding of potential challenges facing multi-domain operations.

Around 17 November 2022, the author was invited to brief Col. Kristen Thompson, commander of the 55 Wing, on the progress of this capstone. The 55 Wing is responsible for several of the Air Force's information warfare and multi-domain operations initiatives. This briefing resulted in several follow-on briefings and operational outputs for the wing. Further, the wing leveraged this research by converting a billet for full-time employment of an information operations officer.

Between 3 December 2021 and 12 December 2021, the author participated in a 16th Air Force working group at the invitation of the 692 ISR Group commander. Small group discussions were had with multiple participants including the group and deputy group commanders. The author out-briefed research-relevant portions of the working group directly to Lt. Gen. Timothy Haugh, the then 16th Air Force Commander.

[152] This chapter is entirely derived from the author's personal notes.

The author participated in the USAF and Joint Artificial Intelligence Center (JAIC) co-sponsored LEAD/DRIVE AI program between 13 December 2021 and 17 December 2021 at the Massachusetts Institute of Technology. This event was the culminating event of a year-long program which identified and trained potential future leaders in the usage of AI. The author held small group discussions with Capt. Shannon Pitts, U.S. Coast Guard Chief of AI, and Chief Master Sergeant Ian Eishen, Senior Enlisted Leader for the Chief of Staff of the Air Force's Strategic Studies Group. The discussions focused on the integration of AI, multi-domain operations, and Operations in the Information Environment.

The author made multiple trips to the greater DC area between 25 January 2022 to 28 January 2022, and 1 June 2022 to 9 June 2022 for discussions with several offices. Highlights of this trip include discussions with Col. Nelson Rouleau in the Office of the Undersecretary of Defense for Policy, members of the Office of the Undersecretary of Defense for Intelligence, multiple members of Checkmate, the Chief of Staff of the Air Force's strategic think-tank, and several Headquarters Air Force offices. The final trip concluded with a small "fire-side chat" event with former Deputy Assistant Secretary of Defense Michele Flournoy and Lt. Gen. (ret.) David Deptula, former Air Force Deputy Chief of Staff for ISR.

On 28 Feb 2022, the author briefed Maj. Gen. Richard Angle, commanding general of 1st Special Forces Command, on the progress of this capstone. In discussions following the briefing, Maj. Gen. Angle provided several inputs to consider related to 1st Special Forces Command's priorities. His most significant input was a new methodology for describing how commander's assume risk for inaction in the information environment. The discussion concluded with some considerations for how multi-domain operations impact the information environment and the role special operations forces (SOF) should play.

The author briefed Maj. Gen. Patrick Roberson, commander and commandant of the U.S. Army John F. Kennedy Special Warfare Center and School, on the progress of this capstone on 10 March 2022. Several other thesis and capstone projects were discussed, and each student or team was given an opportunity to answer or ask questions to the general. For this capstone, the most significant discussion with Maj. Gen. Roberson focused on how U.S. Army special forces could leverage space and cyber capabilities as a part of multi-domain

operations. Considerations were given to when SOF should consider itself the supported unit and when SOF should be supporting space or cyber forces instead.

Topics relevant to this capstone were briefed to and discussed with Lt. Gen. Matthew Glavy, Deputy Commandant of Information, United States Marine Corps, on 24 March 2022. The discussion was had in the context of a Naval Warfare Studies Institute exercise. Various considerations were able to be leveraged from the discussion for the purpose of this capstone, especially pertaining to the intersection of information warfare and multi-domain operations.

Between 3 April 2022 and 9 April 2022, the author provided research briefings and had small group discussions with USSOCOM's Trans-Regional Web Initiative. This research trip was sponsored by Lt. Col. Steve Raymer, the organization's director of science and technology. The trip primarily focused on implementation of USSOCOM's data strategy within the unit and its implications for multi-domain operations. Research for the capstone benefited greatly from a greater awareness of data-related challenge and opportunities. The trip also resulted in creation of the Trans-Regional Web Initiative's data strategy, which was briefed to the unit's commander.

On 12 April 2022, the author had a small in-person discussion with Vice Adm. (ret.) TJ White, former commander of U.S. Fleet Cyber Command. The discussion focused on the intersection of multi-domain operations, information warfare, and operations in the information environment. Most significant from this conversation was an understanding of how USCYBERCOM could leverage multi-domain operations in the future, especially for the purposes of Phase 0 or competition activities.

From 1 June 2022 to 9 June 2022 the author travelled with multiple NPS and USAF members to USINDOPACOM headquarters and Special Operations Command – Pacific (SOCPAC). This trip was performed at the invitation of Maj. Gen. Joshua Rudd, the then SOCPAC commander. Small group discussions were had with multiple staff directorates of both commands. The results of the discussions informed how the commands may leverage the research for ongoing operational challenges and provided inputs to the capstone's considerations.

Between 21 June 2022 and 25 June 2022, the author participated as a panelist for the Phoenix Challenge II conference. The author's research was presented in the context of how to leverage the information environment to deter near-peer adversaries of the United States. Co-panelists of the author included Maj. Gen. (ret.) Chris Ballard, former Deputy Director of Operations at the National Security Agency, and Dr. Austin Long, Deputy Director for Strategy at the Joint Staff. Small group discussions were held with Lt. Gen (ret.) Lori Reynolds, NPS Information Chair, Col. David Acosta, member of the Joint Staff J7, Col. David O'Neil, 16th Air Force J39, and the director of Headquarters Air Force A326K, Col. Christopher Budde. These discussions included future considerations for the development of a USAF information warfare squadron capable of integrating into multi-domain operations.

On 19 July 2022, the author briefed Dr. Wendy Walsh, SES, on this capstone's implication for USAF operational planning practices. As the chief learning officer of Air Education and Training Command, Dr. Walsh is responsible for developing current and future training doctrine for the USAF. This briefing led to several follow-up discussions on how the USAF could refine operational planning with consideration to multi-domain operations. The author was invited to brief a panel of General officers in late September on this capstone but was unable to do so due to conflicting schedules.

V. SUMMARY AND CONCLUSION

The concept of multi-domain operations holds both opportunities and challenges for the joint force. While the U.S. Army and USAF in particular have developed competing visions of multi-domain operations, it is possible for future iterations of doctrine to be more synergistic and aligned with one-another. This capstone worked towards that goal as an annotated bibliography focusing on readings which could suggest doctrinal changes that better align U.S. Army and USAF concepts of multi-domain operations. To this end, the annotated bibliography focused on readings related to deterrence theory and multi-domain operations writ-large. Areas where future U.S. Army and USAF multi-domain operations doctrine may better align include service responsibilities regarding key tenets, the standardization of technology, and the integration of deterrence theories.

A. DETERRENCE THEORIES

This capstone analyzed deterrence theories including conventional deterrence, nuclear deterrence, and cross-domain deterrence. The theories were analyzed in terms of their applicability to multi-domain operations doctrine and in the context of integrated deterrence. Given that integrated deterrence has no solidified definition, these theories are potentially beneficial in developing multi-domain operations' contribution to deterring near-peer adversaries.

Conventional deterrence is must useful in its treatment of deterrence by punishment versus denial, and the interaction of PGMs and achieving conventional deterrence. By differentiating between punishment and denial, conventional deterrence theory supports a more dynamic multi-domain operations doctrine that can deter across different states of competition or conflict. Multi-domain operations doctrine must consider which form of deterrence is the goal and continually re-assess plans to ensure they are consistent with that goal. Further, conventional deterrence's treatment of PGMs offers insight into how modern joint fires can contribute to deterrence outcomes.

Cross-domain deterrence was analyzed, especially in the context of cyberwarfare. Most important in investigating these readings is differentiating between theories of

deterrence which apply to a single domain, such as deterring cyber warfare with cyber warfare, and those which are able to "cross" domains, such as cyber warfare deterring other forms of warfare. Although both are useful for understanding modern forms of deterrence by denial and punishment, theories which focus on a single domain are incongruent with multi-domain operations as a concept. Therefore, cross-domain deterrence is most useful for suggesting doctrinal changes to multi-domain operations.

B. MULTI-DOMAIN OPERATIONS

Following deterrence theory, this capstone focused on analyzing readings which were themselves focused on multi-domain operations. There exists a large variance between readings in how they handle the topic. Further, a distinct difference was highlighted between the U.S. Army and USAF conceptions of multi-domain operations. This difference is addressed through the recognition of "key tenets" within each concept. For the U.S. Army, this is an emphasis on long-range fires and the A2/AD problem-set. For the USAF, the key tenet is command and control with an emphasis on technological empowerment. Both service concepts include the key tenets of influencing populations and integrating non-kinetic fires. All of the key tenets were cross-referenced with integrated deterrence as stated by the 2022 NSS to ensure a direct connection to develop a connection between multi-domain operations and integrated deterrence. Through this analysis, future practitioners may be able to leverage these readings when developing multi-domain operations doctrine.

Analysis of the development of U.S. Army multi-domain operations through specifically selected readings showed that the concept's unique key tenet is long-range fires. These readings include the U.S. Army TRADOC's pamphlet on multi-domain operations, writings concerning the history of U.S. Army multi-domain operations, and analysis of the U.S. Army's new multi-domain operations task force. The key tenet of long-range fires can be seen across the writings as a core, unifying concept. Understanding this enables practitioners to engage in a deeper reading of multi-domain operations documents which relate to the U.S. Army and helps prevent potential confusion with other service multi-domain operations doctrine.

Analysis of the development of USAF multi-domain operations through specific readings was similarly useful in identifying a key, unique key tenet of command and control. Readings discussed which can suggest doctrinal changes include historical USAF documents such as the 2030 Flight Plan and 2035 concept for future operations, and documents written by current practitioners such as those provided by Maj. Kim Nettis or the LeMay Doctrine Center. In addition to their focus on command and control, it is worthwhile to recognize USAF multi-domain operations' emphasis on the integration of technology as an enabling factor.

C. OPPORTUNITIES FOR ALIGNMENT

This annotated bibliography identifies readings which can suggest doctrinal changes to better align U.S. Army and USAF concepts of multi-domain operations. These doctrinal changes include setting roles and responsibilities for key tenets, synchronizing technological developments, and articulating deterrence goals throughout the phases of operations. While both services' concepts of multi-domain operations will continue to evolve, these three areas represent opportunities where evolution could be synergistic based on the readings discussed.

1. Key Tenets

Although both U.S. Army and USAF multi-domain operations include long-range fires and command and control, both place different weights onto these efforts. Working together to delineate responsibilities for these key tenets could alleviate service tensions and result in a more efficient, successful multi-domain operations doctrine for the joint force. For example, given the U.S. Army's focus on long-range fires, USAF multi-domain operations could choose to give more responsibility to the U.S. Army as lead for dictating the role of long-range fires in multi-domain operations. Conversely, the U.S. Army could give USAF lead for developing command and control mechanisms for multi-domain operations.

Both service concepts of multi-domain operations have key tenets of influencing populations and integrating non-kinetic fires. Unlike the first key tenets, which are clearly

delineated between the two services, these key tenets feature significant overlap and are not necessarily unique. Further research should be done which identifies which service should take responsibility for one or both of these key tenets. One possibility may be combining them with other key tenets. For example, the USAF's role in integrating non-kinetic fires as a part of multi-domain operations may focus on the command and control aspect. Similarly, the U.S. Army may take responsibility for a long-range fires style of integrating non-kinetic fires to multi-domain operations. A similar construct could be used for aligning the role of influencing populations within doctrine.

2. Standardization of Technology

One point of contention mentioned throughout the readings is the technological backbone which supports multi-domain operations. For every service, a different project or initiative exists which purports to standardize the hardware components which enable multi-domain operations. Standardizing the technology used for multi-domain operations is one place where the U.S. Army and USAF could better align their efforts. It should not be revelatory that the services should standardized technology to increase their interoperability. However, the readings analyzed in this capstone suggest that placing the standardization of technology in the responsibilities of any one service is not a current priority. Future practitioners will be better able to align U.S. Army and USAF multi-domain operations concepts by designating one service as the responsible agent for developing technological standards.

3. Deterrence Goals

All of the selected readings emphasize, in one manner or another, the ability of the services to deter adversaries or succeed in conflict against them. As the readings on deterrence theory suggest, multiple avenues exist to deter adversaries – but all require cohesion between the deterring forces. In order for multi-domain operations to be successful in deterring adversaries, it must be performed with consistent deterrence goals across the joint force and developed specifically for the current operational context. Both U.S. Army and USAF multi-domain operations concepts could be better aligned on their approach to choosing and fulfilling deterrence strategies. This could be performed by

leveraging the key tenets given their consistency with the requirements of integrated deterrence.

D. FUTURE RESEARCH

Future practitioners and researchers should use this capstone to better align U.S. Army and USAF concepts of multi-domain operations. This can be done through leveraging the readings identified and any analysis of these readings which was performed. This includes both the analysis of specific deterrence theories and their applicability to multi-domain operations and integrated deterrence, and the various understandings of multi-domain operations provided based on services and key tenets. Possibilities of alignment include services being responsible for specific key tenets, creating hardware and technology standards, and more clearly defining the role of deterrence in multi-domain operations doctrine.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. INFORMATION OPERATIONS – THE NEGLECTED CORNERSTONE IN STRATEGIC COMPETITION AND INTEGRATED DETERRENCE

This essay was originally submitted as part of the U.S. Naval Institute 2021 Information Warfare Essay Contest.

The ongoing resurgence of information warfare and operations in the information environment (OIE) by the Sea Services and the joint force will be instrumental to achieving success in strategic competition.[153] Information can be spread as a main effort or as the consequence of another action; its proliferation can be intentional or unintentional; it can be spread overtly, covertly, or clandestinely; and it can affect all audiences from the civilian public to specific adversary military leaders. However, the current framework for these capabilities is lacking.

Based on today's expansive and rapidly changing information environment, there is no effective method for integrating information and influence into the joint planning process. The utilization of influence operations is further hamstrung by no-longer appropriately restrictive U.S. code and CJCSIs, a lack of standardized structure and career potential for information professionals, and disfunction in National Defense Authorization Act language (NDAA). Advocating for consistent language and increased funding for influence operations through the NDAA will drive the joint force towards standardizing their informational professional career field structures and the accompanying processes for integrating information into joint operations. As part of integrating information into joint operations, a new model is warranted which demonstrates clearly how information can be used to influence potential audiences to support a combatant commander's objectives.

[153] Author's Note: The DOD and interagency communities have varying terms to refer to the use of information to influence target audiences to include language based on capability, intent, and type of target audiences. These terms interchangeably include information operations, information warfare, operations in the information environment, psychological operations, and more. While this article will propose solidifying language, it will not recommend what language to use since that has been covered extensively by other authors.

Unfortunately, a historical overview of information in national security drains any enthusiasm from the topic. Using information to achieve national goals under its many titles – such as information operations (IO), psychological operations (PSYOP), strategic communications, and political warfare, to name just a few – has never consistently held the attention of the American defense apparatus. Past attempts to pique the interest of the DOD and Congress include the Navy's WW2 PSYWAR program under then-Captain Zacharias Taylor, the post-WW2 National Psychological Strategic Board, the Cold War's Active Measures Working Group, and the now-defunct United States Information Agency.[154] All of these organizations existed only for limited times where they were able to perform their daily duties but were ultimately disbanded as the spotlight upon using information as a tool shone elsewhere. As recently as 1985, 1990, and again in 2000, various DOD organizations produced recommendations for how the federal government should organize, support, and leverage psychological and information power capabilities.[155] To this date, the most prominent recommendations proposed have not yet been implemented.[156]

If the United States placed a priority on psychological or informational power, that priority would answer critical questions surrounding risk to personnel, prioritization of adversary informational targets, and appropriate responses to malign adversary information operations during peacetime. As it stands, any scholar or practitioner of IO could tell you that we cannot answer these questions – and we don't even agree on where to start.

---

[154] Patrick Porter, "Paper Bullets: American Psywar in the Pacific, 1944–1945," *War in History* 17, no. 4 (2010): 479–511, https://www.jstor.org/stable/26070823; Scott Lucas, "Campaigns of Truth: The Psychological Strategy Board and American Ideology, 1951–1953," *The International History Review* 18, no. 2 (1996): 279–302, https://www.jstor.org/stable/40107707; Fletcher Schoen and Christopher J Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Strategic Perspectives*, n.d., 168, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf; Nicholas J. Cull, The Decline and Fall of the United States Information Agency: American Public Diplomacy, 1989–2001 (Springer, 2012); Nicholas J. Cull, The Decline and Fall of the United States Information Agency: American Public Diplomacy, 1989–2001 (Springer, 2012)

[155] Defense Science Board Task Force, "The Creation and Dissemination of All Forms of Information in Support of Psychological Operations (PSYOP) in Time of Military Conflict," accessed December 31, 2021.

[156] "DOD Psychological Operations Master Plan March 1990." accessed December 31, 2021.

At the same time, national conversation around psychological or informational power is tinged with urgency. Recently, the position of the Principal Information Operations Advisor was created, the State Department has added more funding to their Global Engagement Center, and the DOD Joint Staff is soon to publish a new doctrine towards the implementation of information in joint operations.[157] At the Defense One Outlook 2022 Summit, Undersecretary of Defense for Policy Colin Kahl emphasized the importance of integration across domains, to include the informational domain specifically.[158] Moving forward, it will be important for this urgency to be matched in direction and scope with a meaningful framework for how information can and should be used in the future fight. This is only attainable if the American defense apparatus overcomes problems in responsibility management and definitions.

A. A DEFINING INFORMATIONAL MOMENT

In at least the past seventy years, the United States has managed to fend-off existential threats despite its inadequate approach to executing informational power. The future will not be so forgiving. Concentration on the Global War on Terror and Counter-Violent Extremist Organization operations has tooled the nation's warfighting apparatus accordingly. Meanwhile, America's rivals invested significantly in psychological and informational capabilities which are having real life impacts – from enabling American deaths through vaccine disinformation to threatening the stability of democracy by promoting extremist action.

In the context of strategic competition and integrated deterrence, the Sea Services face recognized and persistent informational threats in the form of Chinese gray zone operations both in the South China Sea and around the globe. It is now common knowledge that these operations leverage economic tradecraft and *fait accompli* to accomplish their

157 "2020 NDAA Brings Cyber, Acquisition, and IT Changes," Defense Systems, accessed December 31, 2021, https://defensesystems.com/2019/12/2020-ndaa-brings-cyber-acquisition-and-it-changes/195063/.

158 "Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Sa," U.S. Department of Defense, accessed December 31, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/.

objectives.[159] One of the most important, but ill-resourced, solutions to this threat requires working with and bolstering partner nations and allies. In the Interim National Security Strategic Guidance, the word "partner" or a variation thereof appears more than 42 times. The use of information as a tool to engage with partners and deter adversaries goes unmentioned: influence is only mentioned four times and only in the context of foreign influence; information is mentioned six times, and only in the context of anti-democratic misinformation and disinformation. It is clear that at the strategic level, information is not yet considered worth investing in as a primary tool for competing with China.

Within the DOD, commonly proposed solutions often fit in one of two categories. First, integrating cutting-edge technologies such as artificial intelligence, unmanned drone swarms, or joint all-domain command and control systems. Second, re-tooling current military operations and capabilities to support competition in innovative ways. At the same time, the joint force has been tasked with leveraging military power to support national objectives – in many cases without the use of kinetic force.[160] It is through this juxtaposition that the Sea Services, in conjunction with the joint force, must re-evaluate what their most effective tools may be and how to use them. One such tool is Operations in the Information Environment (OIE), a concept being driven by the Marine Corps and the Air Force.[161]

The current push towards OIE presents a framework and opportunity for elevating informational power through the integration of cutting-edge technology, the re-tooling of current military operations, and the joint force's implementation of the information function. A joint USMC memorandum signed January of 2020 defined OIE as "actions taken to generate, preserve, or apply military information power in order to increase and protect competitive advantage or combat power potential within all domains of the

[159] Peter Layton, "The Evolving Risk of China's 'Gray Zone' Operations," The Maritime Executive, accessed December 31, 2021, https://www.maritime-executive.com/editorials/the-evolving-risk-of-china-s-gray-zone-operations.

[160] "DOD Strategy for Operations in the IE" accessed December 31, 2021, https://dod.defense.gov/Portals/1/Documents/pubs/DOD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

[161] Dr Sandeep Mulgund, "Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment."

operational environment."[162] The definition includes seven tasks and six capability areas, to include influencing, deceiving, and informing target audiences. The Marines account for discrepancies in intra-service terms, such as the Navy's "use of the term Information Warfare as a subset of actions within a broader OIE construct." The OIE initiative is an opportunity for the services to incorporate psychological and informational power in a more coherent and effective manner than has been achieved before.

B. A SOLUTION MOVING FORWARD

The DOD and U.S. government writ-large has struggled for decades on how to appropriately incorporate information as a tool of national power due to the interconnectivity between all government actions. Information generated by any U.S. government action interacts with audiences relative to any other portion of the U.S. government, whether they be friendly, neutral, and adversarial. Given the expansive and pervasive nature of information, the Sea Services must work with the joint force to implement an operational model which accounts for the recommendations listed by OIE.

While the current Joint Publication 3-13 *Information Operations* and related documentation discusses a high-level relationship between information, potential audiences of interest, and commander's objectives, there still does not exist a model which explains *why* potential audiences might matter to a commander's operations.[163] The existing gap between subject and meaningful implementation is partly responsible for spurious discussion on the importance and prevalence of the information environment, but does not address how and when the information environment is important and for what specific reasons. It is easy for scholars to note the importance of information; it is difficult to explain in concrete terms why that importance exists.

A working model for IO addresses several key areas in simplistic terms, drawing heavily from the joint planning process. First, national-level guidance should inform a

---

[162] "Definitions for Information Related Terms - JOINT MEMORANDUM," accessed December 31, 2021, https://mca-marines.org/wp-content/uploads/Definitions-for-Information-Related-Terms-JOINT-MEMORANDUM-22-JAN-2020.pdf.

[163] Joint Staff, "Information Operations," accessed December 31, 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

center of gravity analysis not only for red forces, but for any institution whose partnership or relationship with the U.S. is of significant importance. Second, the role potential audiences can play in driving the operations of an impactful institution. For example, if the United States is looking to increase partnerships with a country that has a very direct democracy influenced tightly by the will of the people, the U.S. would benefit significantly from first acknowledging that reality and then taking the time and resources to understand the history, culture, and needs of local populations.

On the other hand, if the partner force in question is being evaluated at the military leadership level, an analysis would focus on how to communicate clearly and effectively to include common lexicon and what faux paus to avoid. While these steps may seem simple, they are not codified in any joint publication driving joint force actions. Finally, a strategic communication plan must be developed for interacting with these audiences which includes significant follow-through and is not tied directly to only one operation but to operations across the entire theater to include preparation for future operations.[164] If IO is not planned with timely and persistent engagement in mind, it will fail.

After developing an understanding of potential audiences of interest and their surrounding infrastructure, an account of informational capabilities should be taken to include which capabilities are the most appropriate and what are the requirements for attaining them. This is where barriers to utilizing psychological and informational power are most evident. While any operation, activity, or investment can be used to influence target audiences, several information related capabilities, or enablers, rise above the others in term of effectiveness. The most common of these within the DOD include mission information support operations (MISO; formerly known as PSYOP), civil affairs, and public affairs. Other common but more technically focused enablers include cyberspace and electromagnetic operations. These enablers can be leveraged to produce and disseminate information to target audiences with their local and cultural nuances in mind

164 Author's Note: Per the JP 3-61 *Public Affairs* and CJCSM 3130.03, I (APEX),

Planning Formats and Guidance, Annex Y - Commander's Communication Synchronization – informs long term communications guidance. However, the common processes for utilizing Annex Y are not robust enough for the modern-day information environment.

so that the messages of the United States are articulated clearly, thoughtfully, and effectively.

C. DRIVING THE SOLUTION USING RESOURCES

Today, the usage of information related capabilities is generally limited by one of three factors, all of which are ultimately driven by congressional policy or resource allocation. These three factors are qualified personnel, authorization in U.S. code, and resource allocation. Although much writing has been done on the idea that information could be complimentary or even dominant in planning joint operations, little serious scholarship exists on how to drive implementation of recommended solutions. Most likely, the route to effective leverage of the informational aspect of military power will begin first by demonstrating how information can support ongoing joint operations, and then by demonstrating how information operations could be a leading and supported effort by joint forces.

First, qualified personnel for the implementation of information are both in short supply and of significantly varying flavors. The effective usage of information operations requires not only understanding how to leverage both technical information capabilities, but also a strong foundation in marketing and strategic communications, cultural nuances, or sociological and psychological principles. While the Navy has MISO duties and fills J39 billets—the staff directorate for information operations planning—they have no dedicated MISO personnel. Instead, these duties are often filled by aircrew, cryptologic warfare officers, or as an ancillary duty. The Marine Corps stands in contrast. On one hand, they now have an enlisted PSYOP career field which heavily mirrors the Army's PSYOP capability. On the other hand, their IO officers are normally sent to the Naval Postgraduate School for a Master of Science in Information Warfare Systems Engineering, and only retained as an IO officer for one payback tour.[165]

[165] Erica De la Parra Gehlen and Frank Smith, "Advantage At Sea Requires Rethinking Influence," War on the Rocks, March 5, 2021, http://warontherocks.com/2021/03/advantage-at-sea-requires-rethinking-influence/.

The Air Force has taken its own self-contradictory path forward. With the much-touted stand-up of 16th AF as the service's Information Warfare NAF, one command has centralized C2 of IO, ISR, Cyberspace Operations, EW, and Weather. In 2017, the Air Force also stood up the Information Operations Officer career field in extremely limited numbers, which focuses both on providing joint IO planning and requires a background in social sciences. With no service-wide strategy for specific implementation, however, USAF IO officers have found themselves undermanned and underutilized. Those within 16th Air Force have begun to take on more of a cyber-enabled IO flavor, while those outsides have found themselves stretched thin as joint planners, OPSEC program managers, or inappropriately as intelligence analysts.[166]

While the Army holds the longest continuous history of PSYOP forces, they too have their own dysfunction. Currently, special operations and conventional PSYOP forces are also separated as active duty and reservist forces, respectively. The former operates under 1st SFC, while the later operates under USACAPOC.[167] To date, neither command has ever been led by a PSYOP officer. Converse to the Air Force, the Army has a separate functional area – FA30 – for Information Operations officers. FA30s generally fill the Army's conventional S39 and J39 requirements, while PSYOP officers oftentimes fill the same position in joint SOF constructs.

The second limiting factor for the utilization of psychological and informational power is the staffing process and its guiding regulations. Regardless of the combatant command or joint task force, IO professionals work together to synchronize and implement their capabilities through what is doctrinally known as the information operations working group hosted by the joint force commander's J39.[168] Because many of the authorities for the utilization of influence and strategic communication authorities require coordination

166 Mark Pomerleau, "Air Forces Engaged in 'Cognitive' Warfare," C4ISRNet, October 14, 2019, https://www.c4isrnet.com/dod/air-force/2019/10/14/what-the-new-16th-air-force-means-for-information-warfare/.

167 Dr. Alfred H. Paddock, Jr. , "The 2006 'Divorce' of U.S. Army Reserve and Active Component Psychological Operations Units | Small Wars Journal," accessed December 31, 2021, https://smallwarsjournal.com/jrnl/art/the-2006-%E2%80%9Cdivorce%E2%80%9D-of-us-army-reserve-and-active-component-psychological-operations-units.

168 Joint Staff, "Information Operations."

with various levels of general officers and senior executives across the DOD and interagency, the staffing process for their approval can be extremely lengthy. This protracted turnaround time often cripples psychological and informational power.

These staffing processes are driven by either Chairman of the Joint Chief's Instructions (CJCSIs) or U.S. Title 10 and Title 50 code. These instructions and codes were developed in a time prior to the advent of the modern information environment, where the timeline for effective communication with audiences has been truncated from years and months to days, hours, and in many cases minutes. These two items combined – the lengthy staffing process and its shroud of bureaucratic regulations – effectively neuter timely, relevant, and effective information operations. It is hard to imagine a naval war where the JFMCC would be responsible for signing off on every weapon being fired, after the plan for firing the cannon worked its way through the staff. Information operations should be no different.

Finally, and most importantly, information operations are significantly weakened by a lack of coherent and substantial funding at the Congressional level. Funding through the NDAA is complicated in two manners: a lack of centralized advocacy and consistent use of language. In general, the most highlighted and funded DOD programs are those which entail major construction costs, or which employ clearly recognizable cause and effects, or both. The Navy's Littoral Combat Ship of the DOD's Joint Strike Fighter program are evidence to that point. It is generally easier for congressional representatives to advocate for the large-bill projects which they anticipate will bring jobs to their districts and which will have easy to measure effects on the battlefield, should battle occur. Unlike these major programs, IO creates smaller, more amorphous program that are difficult to directly correlate over the long term and does not result in years-long, massive spending schedules. These factors have caused a significant lack of advocacy at the congressional level. Ironically, IO should be in higher demand given that it can achieve comparable strategic affects to kinetic capabilities, but at a much lower price tag.

The second complicating factor for the NDAA is language. Within the FY22 NDAA, both information operations and information warfare are used distinctly and interchangeable, both in reference to friendly force and adversary use of information to

achieve effects.[169] IO is generally used when referring to the utilization of artificial intelligence and measuring effects in the Information Environment. Information warfare is generally used to refer to adversary disinformation or misinformation efforts, some specifically in relation to gray zone operations. For NDAA funding to psychological and informational power to be effective, it must adopt a common naming schema which will have a two-part effect. First, it will fund more effective and dedicated OT&E of informational forces and drive a command structure to utilize those funds effectively. Second, it will force a standardization of information-related lexicon as words must match their congressional counterparts in order to be eligible for funding.

D. CONCLUSION

Information and psychological operations present a new and effective method for the Sea Services to engage in strategic competition beneath the threshold of armed conflict. Beginning with the NDAA, funding for IO needs to be significantly improved, to include IO forces and technology, which in turn will help drive the development of appropriate service OT&E structures and common doctrinal lexicons. This improved force will develop and drive the utilization of an informational model which informs commanders exactly how information can be used to achieve their objectives, from the tactical to strategic levels. By integrating these advances with Navy information warfare and Marine OIE initiatives, the Sea Services can posture themselves to effectively engage in strategic competition and integrated deterrence and maintain maritime superiority across all domains of conflict.

[169] U.S. Congress, National Defense Authorization Act Fiscal Year 2022. 18 October, 2021.

APPENDIX B. "BREAKING OUT OF OUR SILOS: HOW TO STRENGTHEN RELATIONSHIPS BETWEEN SERVICE-SPECIFIC INFORMATION OPERATIONS COMMUNITIES, AND WHY WE NEED TO"

This essay was originally published by the Modern Warfare Institute at West Point and was co-authored with Capt Don Gomez, U.S. Army.[170]

In the past few years, joint force and interagency leaders have increasingly emphasized the growing importance of information warfare.[171] The U.S. military services have each made strides toward updating doctrine, procuring the right equipment, and reorganizing force structure to better compete with our adversaries.[172] The Joint Staff is working to publish JP 3-XX, which will define the joint lexicon of operations in the information environment (OIE), information warfare (IW), and the roles and responsibilities of the services both for organizing, training, and equipping their OIE forces as well as how to employ them.[173]

While these strategic updates are important and will assist in ensuring that the joint force plans and executes operations from a point of shared understanding, there are activities and initiatives that can be done now to ensure that we are best postured to compete globally.

---

[170] Robert Stelmack and Don Gomez, "Breaking Out Of Our Silos: How To Strengthen Relationships Between Service-Specific Information Operations Communities, And Why We Need To" (West Point, NY: Modern War Institute). https://mwi.usma.edu/breaking-out-of-our-silos-how-to-strengthen-relationships-between-service-specific-information-operations-communities-and-why-we-need-to/.

[171] Mark Pomerleau, "Who should lead the Pentagon's information operations efforts?" C4ISRNET (May 2021). https://www.c4isrnet.com/information-warfare/2021/05/03/who-should-lead-the-pentagons-information-operations-efforts/?

[172] "Information Environment: DOD Operations Need Enhanced Leadership and Integration of Capabilities" Testimony Before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives. (April 2021).

[173] Authors' Note: While information warfare as a term has been in use for decades and has seen an uptick in use recently, it remains an undefined term in joint doctrine. Similarly, information operations has a joint definition, but the services offer their own definitions as well. JP 3-XX is set to establish the joint terms for OIE, IW, and IO, and to encourage the services to adopt similar language. The Air Force is currently set to revise its service definitions toward the JP 3-XX definitions.

Despite the popular image of electrons flowing through cyberspace, IW is inherently a human endeavor, and getting the best minds together in the same room is the responsibility of commanders everywhere. Strengthening the relationship between information warfare professionals spread across the military services by leveraging formal and informal relationships is an easy and cost-effective way to increase our competitive advantage. While each service retains specialists, equipment, and knowledge spanning the spectrum of information-related capabilities, this article will focus on the Air Force's relatively new 14F information operations (IO) officer, the Army's psychological operations (PSYOP) 37 series, and the Army's FA30 (information operations) functional area.

It may come as a surprise to some that the Air Force possesses an information operations capability. Understanding the history behind the Air Force specialty code 14F's recent establishment demonstrates why its development is so significant.[174] While U.S. Army PSYOP forces and their capabilities are by no means new, the youth and size of the Army's PSYOP branch relative to the Army as a whole means that the shared knowledge within the joint force about the unique capabilities of modern Army PSYOP forces remains quite low.

Many of the changes that are currently happening to information operations capabilities are a direct result of the military's strategic shift toward great power competition.[175] The Department of Defense is engaged in persistent competition, and in order to gain and maintain a competitive advantage, the U.S. military must be prepared to meet our adversaries wherever and however they operate. Even though the tools and capabilities utilized for competition are important, nothing will ever subsume the criticality of investing in human capital. It is our hope, by highlighting the many opportunities to cut through imaginary barriers across the services in this article, that we can collectively

[174] Trevor Tiernan, "First Class of Information Operations Airmen Completes 14F Initial Skill Training Course" 67th Cyberspace Wing Public Affairs. (Dec 2020). https://www.nellis.af.mil/News/Article/2450199/first-class-of-information-operations-airmen-completes-14f-initial-skills-train/

[175] "Renewed Great Power Competition: Implications for Defense – Issues for Congress" *Congressional Research Service*. (March 2021). https://news.usni.org/2021/03/09/report-to-congress-on-great-power-competition-and-national-defense-5

invigorate cross-service cooperation and ultimately improve the effectiveness of the U.S. military's information warfare efforts.

A. SO . . . THE AIR FORCE DOES INFORMATION OPERATIONS?

In May 2018, the U.S. Air Force established the IO badge, designed for those in the Air Force specialty code 14F. IO officers integrate physical and informational Air Force capabilities to influence target audiences or adversary decision making, including specialization for leveraging PSYOP, military deception, and operations security. What makes a 14F unique among both Air Force and joint force peers is the occupation's particular focus on the social sciences. It is a firm requirement that 14Fs hold a degree in a social science, like behavioral science or anthropology. The Air Force believes that academic expertise enables 14Fs to better integrate target audience personal, cultural, and cognitive biases into planning, whether the target audience is a specific adversary decision maker or a neutral third-party audience.

Today, 14Fs are responsible for executing three specific mission types. The first, and most common, is at the air operations center (AOC). The AOC is the beating heart of the joint forces air component commander while in theater, fulfilling a similar role to a joint operations center. It is through the AOC that the Air Force plans and executes air operations. Although each AOC is organized in a similar way, every AOC includes its own unique mix of an information operations team (IOT) and an influence operations cell within the IOT. It is also common to find the influence operations cell manned entirely by 14Fs and possibly find the IOT being led by one too. The IOT coordinates cyberspace operations, space, electronic warfare, and intelligence, surveillance, and reconnaissance (ISR) planners to enable cohesive non-kinetic operations. In addition to those functions, many combatant command and major command J39 billets—traditional IO staff directorates—are being filled by 14Fs as well.

The second major mission for 14F officers is within special operations units. You may find 14Fs using their talents to combat disinformation through Joint Task Force Indo-Pacific, where adversaries "continuously sow" disinformation to achieve their regional

objectives.[176] Another point of interest would be U.S. Special Operations Command's new joint military information support operations (MISO) WebOps Center, where 14Fs leverage their social-science academic backgrounds to more effectively "address the opportunities and risks of the global information space."[177]

The final mission for 14F officers is manning the various continental US-based reachback units, like those found within 16th Air Force, the Air Force's first information warfare component numbered air force. The organization combines cyberspace operations, electronic warfare, IO, ISR, and weather in order to present information warfare capabilities and solutions to the various geographic combatant commands, with an emphasis on reducing the information stovepiping that is common among the various information-related capabilities in the military and interagency.[178] Of particular note is the information warfare cell, which has been integral to providing IW and other information-related capabilities, with a particular emphasis on cyber-enabled MISO.[179] Although a relatively recent development in terms of Department of Defense years, 16th Air Force has set the standard for what information operations and strategic communication should look like for the Air Force, and 14Fs have been a core part of that work.

So, yes, the Air Force "does" IO and does it well. The unique education requirements for the Air Force's 14Fs combined with planning and executing operations that emphasize leveraging the cognitive domain, and career-enhancing opportunities (e.g., advanced education and the Education with Industry program) make the Air Force 14Fs unique and valuable members of the joint force's IW roster.

---

[176] Mark Pomerleau, "Special Operations team in Pacific will confront Chinese information campaigns" C4ISRNET. (Mar 2021).

[177] "Statement Of General Richard D. Clarke, U.S. Army Commander United States Special Operations Command Before The House Armed Services Committee Intelligence, Emerging Threats And Capabilities Subcommittee" Congressional Testimony. (April 2019).

[178] Tobias Naegele, "16th Air Force Is Fully Up and Running," Air and Space Forces Magazine (July 2020). https://www.airandspaceforces.com/16th-air-force-is-fully-up-and-running/

[179] Timothy Hague, Nicholas Hall, and Eugene Fan, "16th Air Force and Convergence for the Information War" *The Cyber Defense Review* (Summer 2020). 29–43.

B. INFORMATION WARFARE WILL PLAY A LEAD ROLE IN GREAT POWER COMPETITION

Great power competition is the latest focus of leaders within the Pentagon. If the great power competition trend began with former President Barack Obama's rebalance toward the Pacific region and continued with former President Donald Trump's focus on the People's Republic of China, it is now solidifying under President Joe Biden.[180] In particular, the White House's Interim National Security Strategic Guidance specifically calls out China as the United States' most aggressive threat and Secretary of Defense Lloyd Austin refers to China as America's "pacing threat."[181] [182]

Using the term great power competition to define interactions between the United States and other global powers may be new, but the rules that define great power competition are not. The most important of those rules—such as nuclear deterrence theory, mutually assured destruction, and a norms-based international world order—are legacies of the Cold War. However, what makes great power competition more dynamic is a renewed emphasis on IW as a means of exercising soft and hard power.

While the purpose of this article is not to join the chorus of voices attempting to define IW—it is important to recognize some of the term's key attributes. For example, any definition of IW will involve new technological developments, such as cyber warfare, social media, and space operations, and some a bit older, like psychological operations or electronic warfare. Definitions aside, one truth remains—leveraging the information function is all about influencing your adversary's decision-making cycle while protecting your own. This is where the critical intersection of IW and great power competition comes into play. The process of influencing adversary decision making was particularly important during the Cold War, where one wrong move could set the world on a crash course toward

180 "FACT SHEET: Advancing the Rebalance to Asia and the Pacific," The White House: Office of the Press Secretary (November 2015). https://obamawhitehouse.archives.gov/the-press-office/2015/11/16/fact-sheet-advancing-rebalance-asia-and-pacific

181 Joseph Biden, "Interim National Security Strategic Guidance" The White House. (March 2021). https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

182 Dan Lamothe, "In Japan, top Biden administration officials attempt to set the tone on China," The Washington Post. (March 2021). https://www.washingtonpost.com/national-security/2021/03/15/blinken-austin-china-asia-allies/

nuclear war. In fear of a small nation-on-nation kinetic engagement driving the Soviet Union and United States into full-on conflict, the preferred methods of competition became those of intrigue and proxy wars—terms that now all fall under competition below the threshold of armed conflict.

The IW revolution is expanding. With it, opportunities to compete under the threshold of armed conflict are becoming increasingly more complicated and pronounced. Influence operations are not limited to leaflets and loudspeakers but can now be expertly delivered directly to the intended target audience with products carefully designed with the assistance of data-driven artificial intelligence. Cyber operations allow adversaries to target nation-states and nonstate actors with deniability. Space operations, which were once the business of a handful of superpowers, now feature a diverse set of players competing for resources and developing never-before-seen capabilities. Whereas the first space race was mostly a battle of prestige, the modern iteration has nation-states competing with multinational companies for limited orbital availability while also fielding new capabilities such as continuous global coverage ISR, satellite-based internet, and more.

Winning in great power competition requires clear strategic vision and direction along with desired end states. Influence operations coupled with new technological capabilities represent the United States' most potent tool to meet end states, all while competing under the threshold of armed conflict. The practice of influencing adversary decision making is complicated and requires disciplined and well-coordinated whole-of-government operations, the integration of kinetic and non-kinetic capabilities, and an understanding of how cognitive factors impact an adversary leadership's decision-making cycle. To conduct IW effectively, the U.S. military must leverage the cadre of professionals who have the multidisciplinary education, experience, and dedication to increase our opportunities for success.

C. GETTING IW PROFESSIONALS IN THE SAME ROOM

While the diversity of IW talent across the joint force is a good thing, we run the risk of stovepiping our information professionals like our intelligence-related capabilities

were stovepiped in the years leading up to the 9/11 attacks.[183] Each military service retains tremendous IW talent. The unique assessment, selection, and training pipelines found across the services leads to diversity of thought. If nothing else, even just the unique qualities everyone brings to the fight based on their respective service's culture enables joint access to potential capabilities and personnel that might otherwise be missed or overlooked. Ensuring that all IW capabilities are communicating, integrating, and operating together will lead to increased chances for success in great power competition.

For its part, the Army retains numerous specialists in the constituent fields of IW—ranging from electronic warfare and cyber operations specialists to graphic illustrators and videographers. Compared to the Air Force's 14F IO officer, it is the Army's 37-series military occupational specialties and FA30 functional area that maintain the most complementary skill sets. Army PSYOP officers and noncommissioned officers and FA30 officers often find themselves in similar roles as their Air Force counterparts—as part of an information operations working group, often as the chief. PSYOP forces, with their focused training in language, culture, and influence practices, are the Army's premier influence agents, exploiting psychological vulnerabilities to gain competitive advantage. FA30 officers are trained in the integration of all information-related capabilities (e.g., MISO, military deception, and PSYOP) and work to ensure information operations are well planned and coordinated to achieve the commander's intent and desired effects. While many of these functions may seem similar, they each require extensive specialized training.

When information professionals from across the services are brought together effectively, they can achieve incredible effects. In practice this cooperation seldom occurs outside of a theater of operation. There are, however, opportunities for joint events throughout a unit's training cycle—usually in the form of joint multinational training exercises like Pacific Sentry in the Indo-Pacific and Eager Lion in Jordan. Recently the Air Force ran its first information warfare test exercise, which included opportunities to

183 "9/11 Commission Report," National Commission on Terrorist Attacks Upon the United States. (August 2004).

synchronize IO, electronic warfare, cyberspace operations, and more.[184] Joint exercises are fantastic training laboratories that develop important lessons learned and shared understanding across the services. While participation in joint training exercises should be encouraged and continued, there are numerous opportunities for smaller-scale cooperation that can be leveraged and sustained over the course of a training year. Repeat exposure to joint force information warfare specialists—and the informal and formal relationships that result—provides IW professionals with a tremendous opportunity to accelerate their effectiveness.

First, missions that normally call for an Army 37 series or FA30 should also consider tasking Air Force 14Fs as well. 14Fs are equally qualified to perform these tasks and also bring a unique skill set and perspective that can enhance IO effectiveness. Additionally, the experience and exposure 14Fs would gain through operating in these roles will lead to increased coordination between joint information warfare professionals in the future.

Second, formal, and informal exchanges should be expanded between the Air Force information operations community and PSYOP units. These include increased attendance at IW-related training courses (like the Army PSYOP Officer Qualification Course, which Air Force 14Fs already attend), participating in unit exercises, and instructor exchanges. The relationships developed between Army PSYOP and Air Force IO officers during these events often lead to additional joint training opportunities during pre-mission training and even to broader collaboration during operational deployments. We can attest to this, having experienced it firsthand.

In reality, interservice coordination is, in large part, driven from the bottom up and requires significant pushing and pulling to connect. Commanders—in both the Army and the Air Force—should strongly incentivize and encourage their IW professionals to seek out, and participate in, joint training opportunities. Units at all levels should routinely invite joint service counterparts to participate in training—even for small unit–level exercises.

[184] Mark Pomerleau, "Air Force held first information warfare test exercises" DefenseNews (May 2021). https://www.defensenews.com/information-warfare/2021/05/19/air-force-held-first-information-warfare-test-exercises/

The nature of information warfare requires collaboration—training in a single-service, siloed environment is unrealistic. Ultimately, the United States must learn to unify and coherently wield its IW capabilities in concert to gain strategic advantage and to win in great power competition, and the first step is to start bringing all IW forces together to foster collaboration and coordination.

Each military service has its own rich history of information warfare and service-specific culture tends to color how IW professionals approach problems in the information domain—and that is a good thing. However, the Department of Defense needs to be more creative and committed to finding ways to bring all IW professionals together in the same room to better leverage the skills of our joint partners if we are to gain advantage over our adversaries in great power competition. Breaking down the imaginary barriers between services and building bridges among the various IW specialties is crucial if our country is going to compete against our near-peer foes in the modern era. To do this, we must focus on growing the information warfare force we need for today, and for the future.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. "IT'S TIME FOR INFORMATION OPERATIONS' 'KEY WEST AGREEMENT'"

A version of this paper was submitted to the *11th Annual Pacific Information Operations and Electronic Warfare Symposium*. A presentation on that version was given with Maj Kelley Jhong, U.S. Army.[185]

On 11 March 1947, the Joint Chiefs of Staff convened at Key West to discuss the future roles and responsibilities of the services. The Second World War had come to an end; the services had grown to encompass significantly overlapping missions and capabilities. In particular, the role of the U.S. Air Force and the future of air power. The Key West agreement, as it came to be known, would delineate and deconflict the roles and responsibilities of the services – eventually becoming codified by President Truman's "Functions Paper" on 21 April.[186]

While it would take time for the services to work through Truman's order, the eventual outcome enabled the services to more effectively resource and train for specific missions. Given the new challenges of the 21st century, the Department of Defense is overdue in tackling that task again – this time with particular reverence to the information domain. On 30 April 2021, Secretary of Defense Lloyd Austin unveiled the concept of integrated deterrence, which focuses on integrating the diplomatic, informational, military, and economic tools of national power.[187] Whereas executive departments exist that primarily leverage the diplomatic, economic, and military instruments of power, an awkward, lingering question has been presented: what does it mean to use the informational tool of national power, and who's in charge of which portions of it?

Today's world looks very different from that of 1947. Under the shroud of nuclear deterrence, direct confrontations between great powers have all but ended and been

185 Robert Stelmack. 2022. "It's Time for an Information Operations 'Key West Agreement." *11th Annual IO & EW Symposium, Joint Base Pearl Harbor-Hickam, HI, Oct 17–21.* Unpublished.

186 Robert Beebe, "The Vital Key West Agreement," *Proceedings* 87 (September 1961).

187 C. Todd Lopez, "Defense Secretary Says 'Integrated Deterrence' Is Cornerstone of U.S. Defense," DOD News (April 2021).

replaced by proxy engagements and intelligence activities. Whereas during the Cold War the two primary contenders led economically separated spheres, today's globalized world order is inherently economically intertwined. Information technology has expanded to the point that nearly all nations – and virtually all people – can interact across the globe. Adversaries recognizing this opportunity have embraced informational threats to the United States, such as influencing our national elections or disrupting our global narrative abroad through social media, impacting our ability to work by, with, and through allies and partners. Increasingly the information domain becomes hotly contested – and the United States sits ill-prepared to utilize information for both competition beneath the threshold of armed conflict and in support of conflict operations.

This uncertainty about the role of information is nothing new. The DOD has struggled to define effectively what it is they would like from information since the inception of the first Information Operations (IO) Joint Publication 3-13 in 1998. In reality, this publication was simply a continuation of decades of confusion within the executive branch on how to best leverage information, embodied by such varied efforts such as the United States Information Agency or the National Security Council Active Measures Working Group. Although these examples vary significantly in scope, size, and duration, each represents an inability of the U.S. government to successfully recognize the need for one or more information-based organizations, partially implement them to varying degrees of success, and then ultimately abandon or dismiss it. In 2003, Secretary of Defense Donald Rumsfeld signed the then-classified "IO Roadmap," which dictated specific tasks for the Department of Defense to better leverage information.[188] These recommendations, while helpful, did not ultimately rectify the DOD or executive branch's tumultuous relationship with information.

A potential remedy for the disorganized approach to Information in the USG would be to emulate the 1947 Key West Agreement. The executive branch of the USG – including the DOD, the State Department, and other departments or agencies which impact or leverage the information instrument of national power – requires such an agreement as it

188 "Information Operations Roadmap," DOD Internal Document. 30 October 2003.

pertains to information. Today, the DOD is again working on a solution – this time under the term Operations in the Information Environment (OIE). This new effort presents an opportunity to diverge from those initial attempts at integrating information in the late 1990s and early 2000s by offering new ways of understanding the roles and responsibilities of the services and executive departments regarding information.

A. WHAT DOES ANYONE MEAN WHEN THEY SAY, "INFORMATION OPERATIONS?"

Most recent discussions on IO, Information Warfare, or OIE define the terms by using what is found in Joint Publication 3-13 Information Operations, using various definitions found in PSYOP doctrine, or by definition based on means (information) and ends (influencing adversary or third party decision making). While all of these definitions are technically accurate, they are also broad to the point of having no utility. As is often lamented by information professionals, if all activities, from dropping a weapon from a jet to releasing a public affairs statement, generate information, then everything could be conceptualized as OIE. This extraneous definition has plagued the whole of government since the inception of information operations. Despite the DOD being tasked in the 2020 National Defense Authorization Act to establish, among other things, a "joint lexicon for terms related to information operations," it has so far been unable to do so.[189]

The primary reason the DOD has been unable to break down the OIE problem set effectively is because the definition of OIE is too broad. An effective "key west" agreement would break down information into distinct but related components which each department or agency could take responsibility for all or certain portions of. Further, it would clarify the use of information in strategy, how to organize and train, and how to fund specific activities and capabilities. Therefore, OIE should be broken down into categories with three particular requirements: first, that the components are broad enough that, in summation, still encompass all activities known today as OIE. Second, the components are so specific that the way they would be employed by strategy, the training required for forces to perform those operations, and the funding needed for those operations would be distinct.

189 "2020 National Defense Authorization Act," U.S. Congress.

To understand what components would make sense, it is essential to consider what roles IO officers currently fulfill. As a broad generalization, IO officers work on commanders' staffs as "integrators" of capabilities to influence target audience decision-making. This typically entails synchronizing the activity between various capabilities on the staff, such as psychological operations, electronic warfare, military deception, operations security, public affairs, kinetic-action, and more. This also includes synchronizing with other service components and other interagency efforts. With that in mind, consider the following proposed components:

First, information as a component of traditional operations and integrated campaigning. Defined by the March 2018 Joint Concept for Integrated Campaigning, integrated campaigning is one of the DOD's primary efforts to redefine the military's approach to operations to support integrated deterrence.[190] Officers training and operating to work under this OIE component would look like today's traditional IO officers. What this component does not include, however, are things such as waging long-term influence campaigns with the long-term goals and assessments in mind.

Second, special information operations (SIO). Special information operations would be defined as activities taken to "influence" the outcomes of events to achieve a military advantage through indirect methods. For example, given the increased pervasiveness of PRC multi-domain threats in the new, more economically and technologically intertwined global operating environment, some commanders must be tasked with operating beneath the threshold of armed conflict. Today, these types of operations are often assigned to IO staff because of their focus on leveraging information to achieve objectives but have a stronger regional and interagency component. They generally require more nuance of the operating environment, authorities that exist outside the DOD, and synchronization of problem sets between the DOD and other departments or agencies. By consolidating authority and responsibility for performing SIO, combatant

190 "Joint Concept for Integrated Campaigning," Joint Publication. (March 2018). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257#:~:text=The%20JCIC%20defines%20integrated%20campaigning,and%20duration%20across%20multiple%20domains.

commanders would be better equipped to task specifically trained and organized forces to tackle and deter adversary grey zone operations.

Finally, the last category is that of strategic communication. Again, similar to the other two, this operations category requires themes, messages, symbols, and stories synchronized across the U.S. government to have a coherent impact. Unlike the other two, however, the organizational structure required to properly incentivize leadership to engage in longer-term planning, execution, and measurement of effectiveness is not found in the organizational structures through which the DOD employs forces. This is specifically important as the manner and timeframe in which military commanders are often measured is not commensurate with the time required and types of outcomes expected of long-term influence campaigns.

Adopting these three components as distinct within OIE would have several significant and demonstrable benefits. First, they would enable more effective discussion on the topic of information by providing appropriately scoped problem sets. For example, it would be much easier to agree upon what a "long-term strategic communication campaign" would look like and who should lead it as opposed to a "long-term information operations campaign," which could have multiple definitions. Second, they would also provide more appropriate categories through which Congress could provide funding and oversight. Finally, they would significantly improve our ability to leverage information as a portion of integrated deterrence. It is much clearer to a commander what they should do when tasked to perform "special information operations to counter malign grey zone activity" instead of "long-term strategic communications to influence theater-wide narratives." Although both may (and should) use overlapping capabilities, they will do so in different manners.

B. POTENTIAL FIRST STEPS

Defining these three categories of OIE will have significant positive ramifications for U.S. IO in terms of national leadership, strategy, resourcing, and execution. This framework makes a discussion of roles and responsibilities across the USG achievable in a way they haven't been since the advent of IO as a general concept. To that end, several

recommendations could effectively leverage the new framework to begin immediately engaging in more effective operations. As the title of this article suggests, the USG should convene a "Key West" style meeting to determine the future of OIE under this new structure. To that end, there are several recommendations such a meeting could consider:

First, the USG should consider integrating the OIE community with the intelligence community. Intelligence is a valuable framework given its overlap across nearly all federal departments. This would have multiple benefits. Similar to information, almost all federal entities use intelligence for their own purposes but must also synchronize their information and activities to be efficient and avoid conflicts. OIE could take the best lessons learned from the decades of experience gained in creating what is now the national intelligence community. Further, OIE already requires a close working relationship, given that OIE primarily works through leveraging up-to-date intelligence. By embedding the OIE community into the IC, trust can be built between the two enterprises so that needless friction is avoided when OIE requires that specific intelligence be "burned." An example of this would be the amount of intelligence released by the United States prior to the Russian "special military operation" to inform the global narrative. Finally, this closer working relationship would make it easier for the IC to analyze and measure the constantly growing information domain in a way that supports OIE specifically. Currently, no entity in the IC is developed specifically for that purpose.

Second, the USG should consider creating an undersecretary of defense for information to lead these efforts. While the FY20 NDAA mandated the DOD create the position of principal information operations advisor, that position has not only gone unfilled but, when filled, may ultimately have too little authority and funding to complete its tasks.[191] A USD for information could again take lessons learned from the ASD I&S framework which effectively manages the intelligence community across the several services and service-like combatant commands, and apply them to the OIE community.

Third, consideration should be given to creating a Joint Interagency Task Force for Information and Competition. Similar to the JIATF-South or West, which synchronize and

191 "2020 National Defense Authorization Act."

execute whole of government operations for counter-drug activity in their respective AORs, a JIATF for information with global responsibilities could effectively synchronize and manage operations that fall under OIE. As services and departments organize under their new responsibilities within the three components of OIE, the JIATF could appoint Joint force commanders or directors to lead each effort, providing an appropriate string of authorities and incentive structures to complete the missions while ensuring synchronization across the greater government. An operations center under such a JIATF could serve as the synchronizing mechanism between OIE operations in an iterative fashion – an improvement over today's often lengthy and cumbersome IO working groups. Such a mechanism would ultimately reduce risk to commanders and enable faster, more effective decision-making for OIE.

Fourth, and potentially most controversially, the DOD should consider moving all long-term influence functions and forces into a new organization, which in turn should receive significantly more funding to meet their already mandated public-facing missions. This would include moving MISO authorities and a significant amount of personnel such as Army and Marine PSYOP forces or Air Force Information Operations forces. As it currently stands, the utilization of MISO is often burdened by the shared responsibilities between State and DOD to execute MISO authorities. More efficient staffing and executing processes can be developed by placing personnel and authorities to execute long-term influence functions under one organization. These forces could, for example, form the foundation of the strategic communications joint force commander under the new JIATF, or be slated to support traditional military operations.

The U.S. finds itself in a new bipolar world order, unlike in the past, where the future of western nations is tied economically and through intense interconnectivity with our peer adversary. Integrated Deterrence presents opportunities for the USG to maintain the global status quo but poses significant challenges to current USG structures. Information can fill many of these gaps, but only if it is leveraged in forward-leaning and innovative ways. By redefining OIE as one of the three categories – information as a part of joint campaigning, special information operations, or long-term strategic communications - the USG can begin the process of effectively organizing, resourcing,

writing appropriate strategies for, and ultimately leveraging information. Holding a "Key West" style agreement for roles and responsibilities under this new model would yield incredible results for the OIE community's future. This Key West agreement should then consider several first steps, such as embedding the OIE community within the IC; appointing an appropriately empowered USD for information, creating a national JIATF for leveraging knowledge; and moving long-term influence functions and forces under a singular, resourced organization. Taking these first steps towards re-defining OIE will not only fulfill congressional requirements under the several previous NDAAs but will also enable the executive government to effectively compete with adversaries in an innovative way necessary for the 21st century.

LIST OF REFERENCES

Air University. "Doolittle Series 18: Multi-Domain Operations." (Maxwell AFB: Air University Press, 2019). https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/lp_0003_multi_domain_operations.pdf

Ashley, Richard. "The Poverty of Neorealism." *International Organization* 38, no. 2 (1984): 228.

Association of the United States Army. "Multi-Domain Task Forces: A Glimpse at the Army of 2035." Report, March 2022. https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035

Austin, Lloyd, "Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command," Speech. April 2021. https://www.defense.gov/News/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/

Awanis, Aramé et al., "State of the Industry Report on Mobile Money" (GSM Association, 2022). https://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_English.pdf

Bagby, Laurie M. Johnson. "The Use and Abuse of Thucydides in International Relations." *International Organization* 48, no. 1 (1994): 131. http://www.jstor.org/stable/2706917.

Bergh, Arlid. "Social Network Centric Warfare – Understanding Influence Operations in Social Media" (FFI-RAPPORT, Norwegian Defence Research Establishment, 2019), 10. https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2623/01194.pdf?sequence=1&isAllowed=y

White House. *National Security Strategy*. Washington, D.C.: White House, 2022.

Black, James, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paillé, and Fiona Quimbre, "Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea." Santa Monica, CA: RAND Corporation, 2022.

Bonds, Timothy M., Joel B. Predd, Timothy R. Heath, Michael S. Chase, Michael Johnson, Michael J. Lostumbo, James Bonomo, Muharrem Mane, and Paul S. Steinberg, "What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?." Santa Monica, CA: RAND Corporation, 2017.

Bradshaw, Samantha. “Influence Operations and Disinformation on Social Media” Centre for International Governance Innovation. November 2020. https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media/?utm_source=twitter&utm_medium=social&utm_campaign=ai-series

Burke, Edmund, Kristen Gunness, Cortez Cooper, and Mark Cozad, “People’s Liberation Army Operational Concepts” (2020), RAND Corporation. https://www.rand.org/pubs/research_reports/RRA394-1.html

Choucri, Nazli. “Cyberpolitics in International Relations,” précis, Spring 2013, 6–10 & 28.

Congressional Research Service. “The Army’s Multi-Domain Task Force (MDTF),” (May 2022). https://sgp.fas.org/crs/natsec/IF11797.pdf

Cordray, Robert and Marc Romanych, “Mapping the Information Environment.” *IO Sphere* (Summer 2005).

Davis, Paul. “Deterrence, Influence, Cyber Attack, and Cyberwar,” International Law and Politics 47, (2015). 347.

Dominiak, Artur and John Bassette, “The Application And Employment Of Special Forces To Effectively Operate In The Multi-Domain Operations Environment Of Large-Scale Combat Operations.” Capstone, Naval Postgraduate School (December 2021).

Doyle, Michael. “Thucydidean Realism.” Review of International Studies 16, no. 3 (1990): 223–37. http://www.jstor.org/stable/20097224.

Enterprise Capability Collaboration Team, “Air Superiority 2030 Flight Plan.” United States Air Force, May 2016.

Fiala, Otto. “Resistance Resurgent: Resurrecting a Method of Irregular Warfare in Great Power Competition” Special Operations Journal, 7:2 (2021). 109–135.

Frank Zagare and D. Marc Kilgour, *Perfect Deterrence* (Cambridge: Cambridge University Press, 2000), 6.

Freedman, Lawrence. “General Deterrence and the Balance of Power.” Review of International Studies 15, no.2 (1989).”

Friis, Karsten and Olav Lysne, “Huawei, 5G and Security: Technological Limitations and Political Responses,” Development and Change 52, no. 5. 1174–1195.

Gady, Franz-Stefan and Alexander Stronell, "Cyber Capabilities and MultiDomain Operations in Future High-Intensity Warfare in 2030," Cooperative Cyber Defence Centre of Excellence (2020). 152.

Gallus, Jessica, Melissa Gouge, Emily Antolic, Kerry Fosher, Victoria Jasparro, Stephanie Coleman, Brian Selmeski, and Jennifer Klafehn. "Cross-Cultural Competence in the Department of Defense: An Annotated Bibliography," U.S. Army Research Institute for the Behavioral and Social Sciences. Special Report 71 (Fore Belvoir, VA: 2014).

Garamone, Jim. "Nominee Says Strategic Command Must Deal With Changing World" U.S. Department of Defense (September 2022). https://www.defense.gov/News/News-Stories/Article/Article/3160085/nominee-says-strategic-command-must-deal-with-changing-world/

Garst, Daniel. "Thucydides and Neorealism." International Studies Quarterly 33, no. 1 (1989): 3–27. https://doi.org/10.2307/2600491.

Gilpin, Robert. "The Richness of the Tradition of Political Realism." International Organization 38, no. 2(1984): 287.

Green et. al., Michael. "Counter-Coercion Series: China-Vietnam Oil Rig Standoff," Asia Maritime Transparency Initiative. June 2017. https://amti.csis.org/counter-co-oil-rig-standoff/

Harrington, Jake and Riley McCabe, "Detect and Understand: Modernizing Intelligence for the Gray Zone" Center for Strategic and International Studies. (December 2021). https://www.csis.org/analysis/detect-and-understand-modernizing-intelligence-gray-zone

Headquarters, Air Force. "Air Force Future Operations Concept: A View of the Air Force in 2035." United States Air Force, September 2015. https://www.af.mil/Portals/1/images/airpower/AFFOC.pdf

Herz, John. "Political Ideas and Political Reality." The Western Political Quarterly 3, no. 2 (1950): 161–78. https://doi.org/10.2307/443481. 161.

Hoffman, Frank and Andrew Orner, "The Return of Great-Power Proxy Wars." War on the Rocks, September 2021. https://warontherocks.com/2021/09/the-return-of-great-power-proxy-wars/

Jervis, Robert. "Dilemmas About Security Dilemmas." Security Studies 20:3 (2011), 416–423.

———. "Review of Deterrence Theory Revisited," by Alexander George and Richard Smoke. World Politics 31, no. 2 (1979): 289. https://doi.org/10.2307/2009945.

Joint Staff. “Capstone Concept for Joint Operations: Joint Force 2020,” Internal report. September 2012.

Joint Staff. “Joint Publication 3-0, Joint Campaigns and Operations,” June 2022.

Joint Staff. “Joint Publication 3-0, Joint Campaigns and Operations,” October 2018.

Joint Staff. “Joint Publication 3-13.2, Military Information Support Operations, Incorporating Change 1,” Joint Staff. December 2011.

Joint Staff. “Summary of the Joint All-Domain Command and Control (JADC2) Strategy,” March 2022. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

Keegan, John. *A History of Warfare* (London: Hutchinson, 1993.) 3.

Keohane, Robert, “Cooperation and International Regimes,” in After Hegemony: Cooperation and Discord in the World Political Economy (NJ: Princeton University Press, 1984).

———. “Realism, Neorealism, and the Study of World Politics,” in Neorealism and its Critics, ed. Robert Keohane (New York: Columbia University Press, 1986), 15.

Kimmons, Sean. “Second Phase of Multi-Domain Task Force Pilot headed to Europe,” United States Army. October 2018. https://www.army.mil/article/212342/second_phase_of_multi_domain_task_force_pilot_headed_to_europe

Koven, Barnett. “Competing with Great Powers through Competitive Strategy and Unconventional Warfare” Special Operations Journal, 7:1, 66–86.

Lacdan, Joe. “Army, Air Force Form Partnership, Lay Foundation for CJADC2 Interoperability,” Army News Service. October 2020. https://www.af.mil/News/Article-Display/Article/2369626/army-air-force-form-partnership-lay-foundation-for-cjadc2-interoperability/

Lebow, Richard Ned. “Thucydides and Deterrence.” Security Studies 16:2 (2007): 166.

Libicki, Martin. *Conquest in Cyberspace* (Cambridge: Cambridge University Press, 2007).

Lindelauf, Roy. “Nuclear Deterrence in the Algorithmic Age: Game Theory Revisited,” in Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century-Insights from Theory and Practice, ed. By Frans Osinga and Tim Sweijs (The Hague: T.M.C. Asser Press, 2021)..

Lindsay, Jon and Erik Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York, NY: Oxford University Press, 2019).

Lupovici, Amir. "Cyber Warfare and Deterrence: Trends and Challenges in Research," Military and Strategic Affairs 3, no. 3 (2011). 49.

Mallory, King "New Challenges in Cross-Domain Deterrence." Perspective. Rand Corporation (Santa Monica, CA: 2018).

Mazarr, Michael, Bryan Frederick, John J. Drennan, Emily Ellinger, Kelly Elizabeth Eusebi, Bryan Rooney, Andrew Stravers, and Emily Yoder, "Understanding Influence in the Strategic Competition with China." Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA290-1.html.

McConville, James. "The Army in Military Competition: Chief of Staff Paper #2." White Paper (March 2021).

McCoy, Kelly. "Competition, Conflict, and Mental Models of War: What you Need to Know About Multi-Domain Battle." Modern War Institute at West Point. January 2018. https://mwi.usma.edu/competition-conflict-mental-models-war-need-know-multi-domain-battle/

———. "The Road to Multi-Domain Battle: An Origin Story." Modern War Institute at West Point. October 2017. https://mwi.usma.edu/road-multi-domain-battle-origin-story/

Mearsheimer, John. *Conventional Deterrence* (New York: Cornell University Press, 1983), Preface.

Morgenthau, Hans, Politics Among Nations: The Struggle for Power and Peace (New York: Knopf, 1954), 4.

Mowery, David C. "Plus ca change: Industrial R&D in the 'third industrial revolution,'" Industrial and Corporate Change, Volume 18, Issue 1, February 2009, 1–50.

Nettis, Kimber. "Multi-Domain Operations: Bridging the Gaps for Dominance," Wild Blue Yonder. (Maxwell AFB: Air University Press, 2020).

Office of Irregular Warfare and Competition, Directorate for Joint Force Development (J-7), "Curriculum Development Guide for Irregular Warfare." Joint Staff, June 2022. 11.

———. "Irregular Warfare Mission Analysis." Joint Staff, October 2021.

Pelleriti, John A, Michael Maloney, David C. Cox, Heather J. Sullivan, J. Eric Piskura, and Montigo J. Hawkins, "The Insufficiency of U.S. Irregular Warfare Doctrine" Joint Forces Quarterly 93, no. 2 (2019). 104–110.

Priebe, Miranda, Douglas C. Ligor, Bruce McClintock, Michael Spirtas, Karen Schwindt, Caitlin Lee, Ashley L. Rhoades, Derek Eaton, Quentin E. Hodgson, and Bryan Rooney, "Multiple Dilemmas for the Joint Force: Joint All-Domain Command and Control." Santa Monica, CA: RAND Corporation, 2020.

Purser, Jennifer. "Multi-Domain Operations and Information Warfare in the European Theater," Military Review (November-December 2020).

Purvis, James. "Traditional and Irregular Warfare: A Flawed Concept for Categorizing Conflict." Joint Forces Staff College, 2009.

Reynolds, Lori and Thomas Rid, "Competing for Influence: Operations in the Information Environment." Podcast. Modern Warfare Institute (January 2021).

Reynolds, Phil "What Comes Next? An Argument for Irregular Warfare in National Defense" Military Review (September-October 2012).

Rid, Thomas and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies 38, no. 1–2, 7.

Schelling, Thomas. *Arms, and Influence* (Connecticut: Yale University Press, 1966).

Secretary of the Air Force Public Affairs, "Air Force to Phase Out 13O Career Field, Strengthen All Airmen Joint Capabilities." Press release, February 2022. https://www.af.mil/News/Article-Display/Article/2938234/air-force-to-phase-out-13o-career-field-strengthen-all-airmen-joint-capabilities/

Seip, Mark. "Bad Idea: All Sensors, All Shooters, All the Time – a Joint All-Domain Command and Control System That Prioritizes Centralization" Defense360 (December 2020). https://defense360.csis.org/bad-idea-all-sensors-all-shooters-all-the-time-a-joint-all-domain-command-and-control-system-that-prioritizes-centralization/

Sinnreich, Richard. "Multi-domain battle: Old wine in a new bottle?" Army, 67(2), 13–14. (2017).

Smith, Grant. "Multi-Domain Operations: Everyone's Doing It, Just Not Together." Other The Horizon: Multi-Domain Operations and Strategy. June 2019. https://othjournal.com/2019/06/24/multi-domain-operations-everyones-doing-it-just-not-together/

Stelmack, Robert, and Don Gomez. "Breaking Out Of Our Silos: How To Strengthen Relationships Between Service-Specific Information Operations Communities, And Why We Need To." West Point, NY: Modern War Institute. https://mwi.usma.edu/breaking-out-of-our-silos-how-to-strengthen-relationships-between-service-specific-information-operations-communities-and-why-we-need-to/.

.Sweijs, Tim and Samo Zilincik, "Cross Domain Deterrence and Hybrid Conflict," Report. The Hague Centre for Strategic Studies (December 2019).

Taylor, P. M. "Perception Management and the 'War' Against Terrorism." Journal of Information Warfare 1, no. 3 (2002): 16–29. https://www.jstor.org/stable/26504100.

Thucydides, The History of the Peloponnesian War, trans. Richard Crawley (New York: E. P. Dutton and Company, Inc., 1950), 1.

Townsend, Stephen. "Accelerating Multi-Domain Operations." Military Review, September-October 2018. (Army University Press, 2018).

Training and Doctrine Command. "TRADOC Pamphlet 525-3-1 The U.S. Army in Multi-Domain Operations 2028," (U.S. Army Training and Doctrine Command, 2018), Preface.

Vasquez, John. The Power of Power Politics: From Classical Realism to Neotraditionalism (Cambridge: Cambridge University Press, 1999), 43–44.

Waltz, Kenneth, *Theory of International Politics* (Mass: Addison-Wesley, 1979).

Webb, Michael and Stephen Krasner, "Hegemonic Stability Theory: An Empirical Assessment." Review of International Studies 15, no. 2 (1989): 183. http://www.jstor.org/stable/20097178.

Wilner, Alex. (2020) "US cyber deterrence: Practice guiding theory," Journal of Strategic Studies, 43:2, 251.

Wilson, Heather, David Goldfein, and Kaleth Wright, "Multi-Domain Command and Control (MDC2) Implementation Plan," June 2018.

Wohlforth, William. "Realism and the End of the Cold War." International Security 19:3 (Winter 1995): 91.

Work, Bob. "Army War College Strategy Conference" (2015), U.S. Department of Defense, https://www.defense.gov/News/Speeches/Speech/Article/606661/army-war-college-strategy-conference/

Wright, Samuel. "Rethinking Boundaries, Spaces, and Networks Between Geography and Military Science: Understanding and Actualizing Real-Time Integrated Command and Control for Joint Air Operations" (2020). Honors Theses. 1473.

Yoho, Keenan D.; deBlanc-Knowles, Tess; and Borum, Randy. "The Global SOF Network: Posturing Special Operations Forces to Ensure Global Security in the 21st Century." Journal of Strategic Security 7, no. 2 (2014): 1–7.

Zagare, Frank and D. Marc Kilgour, Perfect Deterrence (Cambridge: Cambridge University Press, 2000), 6.

———. "A Re-examination of the Logical Foundation of Deterrence Theory." Journal of Theoretical Politics 16, no. 2 (2004). 107.

———. "Classical Deterrence Theory: A Critical Assessment." International Interactions 21, no. 4 (1995).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California