Operations in the Information Environment: Achieving Decision Dominance

A Monograph

by

Lieutenant Colonel Megan N. Davis
US Air Force

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

2021

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
27-05-2021	MASTER'S MONOGRAPH	JUNE 20 – MAY 21

4. TITLE AND SUBTITLE
Operations in the Information Environment: Achieving Decision Dominance

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lt Col Megan N. Davis, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ADVANCED MILITARY STUDIES PROGRAM

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The changing character of warfare necessitates that Operations in the Information Environment (OIE) be at the forefront of military planning and execution. With an inability to match US physical power, US adversaries rely increasingly on asymmetric approaches that include information warfare capabilities to undermine US actions and influence. Future Joint All Domain Operations (JADO) will require an integrated and interdisciplinary approach to warfighting. This paper asserts that deliberate action taken to target the enemy's cognitive and information filters will impede the adversary's decision-making process and deprive him of the ability to make informed decisions about effectively employing military power. By examining Russian operations in the information environment, information warfare activities, and the theory of Reflexive Control, the author has developed the Theory of Decision Dominance. This theory seeks to provide a way to deliberately use information to target an adversary's behavior and information systems. The goal is to deny the adversary the ability to perceive and recognize the situation and hinder his ability to effectively use the information presented to him to make calculated decisions.

15. SUBJECT TERMS
Information Environment, Information Advantage, Decision Dominance, Reflexive Control, Information Warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Megan N. Davis
(U)	(U)	(U)	(U)	46	**19b. PHONE NUMBER** *(include area code)* 913 758-3300

Monograph Approval Page

Name of Candidate: Lieutenant Colonel Megan N. Davis

Monograph Title: Operations in the Information Environment: Achieving Decision Dominance

Approved by:

____//Signed/9 March 2021/JKG//_____, Monograph Director
James K. Greer, PhD

____//Signed/9 March 2021/MJY//_____, Seminar Leader
Matthew J. Yandura, COL

//signed 20 APR 21/BAP//, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 20th day of May 2021 by:

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

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

Abstract

Operations in the Information Environment: Achieving Decision Dominance, by Lt Col Megan N. Davis, 42 pages.

The changing character of warfare necessitates that Operations in the Information Environment (OIE) be at the forefront of military planning and execution. With an inability to match US physical power, US adversaries rely increasingly on asymmetric approaches that include information warfare capabilities to undermine US actions and influence. Future Joint All Domain Operations (JADO) will require an integrated and interdisciplinary approach to warfighting. This paper asserts that deliberate action taken to target the enemy's cognitive and information filters will impede the adversary's decision-making process and deprive him of the ability to make informed decisions about effectively employing military power. By examining Russian operations in the information environment, information warfare activities, and the theory of Reflexive Control, the author has developed the Theory of Decision Dominance. This theory seeks to provide a way to deliberately use information to target an adversary's behavior and information systems. The goal is to deny the adversary the ability to perceive and recognize the situation and hinder his ability to effectively use the information presented to him to make calculated decisions.

Contents

Acknowledgments

I would like to thank my Air Force friends, Bri Peterson and Tammy Nykun, as well as my parents, Ron and Teresa Mallare, for their review and recommendations during the writing process. I would also like to thank my husband, Major Justin Davis, who helped me focus my topic, research, and use of specific terminology to make this paper beneficial to Air Force concept development. He is a wonderful husband, father, officer, and mentor. Additionally, Dr. Sandeep Mulgund (Headquarters Air Force) provided his expertise and critical review of my research and findings. For this, I am very grateful. Dr. Greer is a fantastic mentor and advisor, and I thank him for his direction and guidance along this journey. Lastly, Col Matthew Yandura' s leadership, creativity and direction empowered me throughout this process. He is one of a kind! The writing of this monograph has been a labor-intensive process but highly rewarding.

Abbreviations

ATO	Air Tasking Order
C2OIE	Command and Control of Operations in the Information Environment
C4I	Command, Control, Communications, Computers and Intelligence
DDoS	Denial of Service
EMS	Electromagnetic Spectrum
ISR	Intelligence, Surveillance, and Reconnaissance
JADO	Joint All Domain Operations
JCOIE	Joint Concept of Operating in the Information Environment
NATO	North Atlantic Treaty Organization
OAI	Operations, Activities, and Investments
OIE	Operations in the Information Environment
USAF	United States Air Force

Figures

Tables

Introduction

Late 20th century and 21st century events demonstrate a highly sophisticated and complex character of warfare in which information and asymmetric methods, enabled by technology resources, secure victory. The evolution in the character of warfare is prefaced on technical advancements that make the reach and power of information more drastic reducing the requirement for physical confrontation; thus, changing the military operating environment. Non-traditional military means, specifically the use of information, necessitate a military force that is agile and adaptable across all domains. Using information and the information environment, adversaries of the United States seek to influence and shape perceptions that create uncertainty and an incorrect understanding of the environment. These efforts propagate discontent, influence decision making, and undermine US interests to achieve the information advantage and prevail across the competition and conflict continuum.

With the Department of Defense's focus on Joint All Domain Operations (JADO), future military concepts, doctrine, and planning must give considerable thought to Operations in the Information Environment (OIE) and the idea of decision dominance. US adversaries have developed and refined their processes to meter escalation while remaining under the threshold of armed conflict. The result of these actions highlights the importance of gaining and maintaining the information advantage. In the future, US military planning will require a deliberate sequence of actions where information targets the adversary's behavior and information systems to deny him the ability to achieve the information advantage and decision dominance (defined on page 5).[1] This monograph will explore the primary research question, "how might the US deny the

[1] Mark Kelly, *Strategic Multilayer Assessment (SMA) on Command and Control of Operations in the Information Environment* (Washington, DC: HAF A3, 2020), 1.

enemy decision dominance?" and seeks to understand how the US military can achieve decision dominance across the competition continuum.

Strengthening the ability of the commander to make rapid and informed decisions underpins modern warfare. In future conflict, the accuracy and speed in which information is received, processed, and used to make decisions will dictate the competitive advantage. The US' adversaries – unable to match US physical power – continue to invest in significant non-traditional military methods, specifically information and other gray zone activities, to undermine US actions. Active measures[2] in the information environment target the cognitive processes of the US government, military, and population with the goal of creating confusion, uncertainty, and disorder. Coupled with cyber operations, these overt and covert measures aim to target information systems, influence behavior, discredit institutions, and paralyze US decision making.[3] This paper asserts that deliberate action taken to target the enemy's cognitive and information filters will impede the adversary's decision-making process and deprive him of the ability to make informed decisions about effectively employing combat power. Achieving information advantage and decision dominance requires pinpointed action in the information environment to set conditions for successful all-domain operations.

The US military must understand the importance of operations in the information environment and the adversary's attempts to exploit it. This understanding will safeguard US interests and enable effective military operations. The information environment includes the cyberspace domain but impacts all other domains, including the air, space, land, and maritime domains. US military strategy and planning must integrate processes in the information environment into broader kinetic and non-kinetic plans across the competition continuum. Doing

[2] Richard H. Schultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy*. (NY: Pergamon Press, 1984), 2. Active Measures (aktivnyye meropriatia) is a term to describe an "array of overt and covert techniques for influencing events and behavior in, and the actions of, foreign countries."

[3] Ibid., 2-3.

so will reduce the adversary's ability to persistently control, manipulate, and manage inputs in the information environment and throughout the gray zone of conflict. Reducing the adversary's ability to act in the information space provides the US with opportunities to gain accurate information, operate with less interference, make informed decisions, and influence outcomes to its benefit. The findings of this study will inform the Joint Force's development of the Joint All Domain Operations (JADO) concept and explore ways in which the US can gain and maintain decision dominance over its adversaries.

As delineated in the 2018 National Defense Strategy, Russia is a strategic competitor and a threat to US interests.[4] Since the 1960s, Russian information warfare activities have supported its national strategy. Through continuous actions in the information environment, Russian information operations aim to manipulate, control, and change the designated population's behaviors. In recent years, Russian operations continue to expand control and to influence operations in the cyber domain. The combination of influence and malicious cyber operations allows the Russian government to manipulate the narrative and achieve political objectives without open conflict. Underpinning Russian information warfare activities is the theoretical approach known as Reflexive Control. This theory asserts that one can affect a designated audience's decision-making process by carefully crafting information, disinformation, or malinformation that causes the adversary to act as the aggressor wants him to.[5] Through this approach, the goal is to deliberately mislead or disrupt the functioning of the adversary's command and control processes. By examining the pillars of Reflexive Control, the US can understand its adversary's tradecraft and develop its own methods to apply in the information environment. Well-planned and deliberate operations in the information environment will deny

[4] US Department of Defense, *Summary of the 2018 National Defense Strategy* (Washington, DC: Government Publishing Office, 2018), 2.

[5] Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 254.

the enemy the opportunity to exploit US decision-making capabilities and provide the US military with the opportunity to manipulate and control the adversary's actions across domains.

The following terms and definitions are presented for clarification and apply to this research and analytical discussion:

- **Information Environment:** the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[6]
- **Operations in the Information Environment:** those activities that generate, apply, and alter information to change or maintain the perceptions, attitudes, and other elements that influence the decisions and behaviors of relevant actors and, in turn, the course of events.[7]
- **Information Warfare:** the employment of military capabilities in and through the information environment to deliberately affect an adversary's human and system behavior and preserve friendly freedom of action during cooperation, competition, and conflict. Information warfare creates multiple dilemmas for the adversary.[8]
- **Information Operations:** the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[9]

[6] US Department of Defense, Joint Staff, Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: Government Publishing Office, 2017), 2-5.

[7] US Air Force, *C2 of Operations in The Information Environment (OIE) Working Group* (Washington, DC: HAF A3, 2020).

[8] Deputy Commandant, Combat Development and Integration, and Deputy Commandant for Information, Memorandum, *Definitions of Information Related Terms* (Washington, DC: Headquarters, US Marine Corps, 2020), 1-2.

[9] US Department of Defense, Joint Staff, Joint Publication (JP) 3-13, *Information Operations.* (Washington, DC: Government Publishing Office, 2014), iii.

- **Information Advantage:** Conditions in the information environment favorable to the achievement of the commander's overall objectives. Such conditions may arise on their own or be the result of deliberately using information to influence relevant actors; inform desired audiences; attack, exploit, and defend information, information networks, and systems; and support human and automated decision-making. Information advantage can exist in the human or systems dimensions of the information environment separately or simultaneously.[10]

- **Decision Dominance:** a desired state in which commanders' sense, understand, decide, and act faster and more effectively than their adversaries.[11] Decision Dominance works within the enemy's decision-making cycle to remove the sanctuary of time and to eliminate options in space.

Given the primary research question, the author hypothesizes that for the US military to prevail in future competition and conflict, it is imperative that the Joint Force better understand how its adversaries operate in the information environment, refine and utilize some of their practices, and develop robust information warfare capabilities and outcomes. The ability to create outcomes will require organizational change and procedural change in joint planning and operations. Information is a source of power. Strategic campaign and operational-level planning approaches must shift to focus on how information affects the operational environment, leverage information to influence the adversary's behavior, and enhance overall military effectiveness, both in virtual and physical domains.

---

[10] US Air Force, *C2 of Operations in The Information Environment (OIE) Working Group*, 3.

[11] US Army Cyber Center of Excellence, *Information Advantage: Expanded White Paper (Pre-Decisional)* (Fort Gordon, GA: US Army Cyber Center of Excellence, 2020), 3-1.

The most significant limitation of this research is the access to primary source documents from the Russian Federation. The theory and strategy of the Russian Federation have been extrapolated from translated and secondary sources. Secondary sources include works from reputable institutions, academic journals, and well-cited books. De-limitations of this study are based on the scope and requirement of the monograph. First, current research focuses on the information environment and implications from past planning and operational execution. This study does not explain how to measure the effectiveness of operations in the information environment. Second, this research does not address current US military operations in the information environment due to classification and the importance of safeguarding US sources and methods. Third, this research focuses on Russian actions in the information environment. The theory of Reflexive Control and associated activities is analyzed to understand how a US adversary operates in the information environment and to provide awareness for future US theory and practice for operations in the information environment. The secondary focus includes understanding the application of information warfare to military operations and a study of current military vernacular to include information advantage and decision dominance. The information environment is one variable of the broader all-domain operations strategy as envisioned by the Joint Warfighting Concept.

Literature Review

The evolving character of war demands that the US military better understand Operations in the Information Environment (OIE) and develop ways to exploit the adversary's efforts within this environment. This discussion will include an understanding of the applicable theory – Reflexive Control – and provide a conceptual and empirical overview of the literature available on information warfare and associated terms. The research will inform the methodological approach and analysis for this monograph and provide a baseline understanding of methods available to deny the enemy decision dominance in competition and conflict.

Following World War II, Russia dedicated a significant amount of time and resources to exploit the information environment both in peacetime and wartime. For more than 60 years, Russia refined its information warfare techniques to target decision-makers and populations' cognitive processes at large. Through the theory of Reflexive Control, Russian information warfare activities demonstrate a robust capability to shape perceptions, attitudes, and decision-making processes. While some Russian actions are focused internally within their borders, external employment seeks to affect a state's decision-making processes through the careful application of tailored information, more commonly referred to as disinformation.[12]

More specifically, Reflexive Control theory is an information warfare means in which the actor aims to convey deliberately prepared (dis)information that forces the targeted audience into making a predetermined decision desired by the originator.[13] This theory deliberately targets a specific person or group. In the early and mid-1900s, several Russian theorists, building upon each other's thoughts and research, advanced the Reflexive Control methods used today. M.D. Ionov, considered one of the first great thinkers on the subject, understood the military value of attempting to control the adversary's cognitive processes. One achieves control and influence through four methods: power pressure or show of force; measures to present false information; influencing the decision-makers processes; and altering the decision maker's time.[14] Nikolay Ivanovich Turko views information as a weapon and articulates how information warfare can be used against information resources to destabilize the opponent and cripple one's decision-making process. S.A. Komov, one of the most well-read authors of the 1990s in Russia, articulates information warfare elements as distraction, overload, paralysis, exhaustion, deception, division,

[12] Schultz and Godson, *Dezinformatsia*, 2, 37-38. Disinformation is "non-attributed or falsely attributed communication, written or oral, containing intentionally false, incomplete, or misleading information (frequently combined with true information), which seeks to deceive, misinform and/or mislead the target."

[13] Thomas, *Recasting the Red Star*, 241.

[14] Ibid., 245.

pacification, deterrence, provocation, and pressure.[15] S. Leonenko further states that information is a weapon in which a specifically selected piece of information can be used to generate changes within an information process of an information system (computer or mind). The aim is to deliberately impact the decision-making of the adversary.[16] His writings move away from the use of the stratagem and replace this method with the idea of denial and deception to influence and control the enemy's cognitive processes. The evolution of Reflexive Control shows the clear intersection between mental processes and the psychological impact of information on decision making.

The application of this theory results in the ability to influence the adversary's combat plans, formations, and force posturing actions and his perception of the situation. Underpinning this theory is the idea of reflex. Reflex is the specific process of attempting to replicate the enemy's cognitive functions, reasoning, and behaviors to generate a condition in which the target makes a decision he thinks is well-reasoned but is the initiator's desired outcome.[17] The filter represents the human mind or computer processor that supports decision-making and allows a commander to separate useful information from inaccurate or irrelevant information. A filter is the "collective image" of the adversary's techniques, tactics, and procedures for organizing, processing, and acting on the information.[18] By replicating information processes and behavior, Reflexive Control allows an actor to target his opponent's filter, resulting in altered decision-making and actions on the battlefield.

As demonstrated throughout history, the ability to make informed decisions is the crux of successful military engagement and operations. As technology increases and the speed at which

[15] Thomas, *Recasting the Red Star*, 249.

[16] Ibid., 247.

[17] Schultz and Godson, *Dezinformatsia*, 38.

[18] Timothy L. Thomas, “Russia’s Reflexive Control Theory and the Military.” *Journal of Slavic Military Studies*, no. 17 (2004): 243.

data transmission increases, it becomes even more imperative to ensure the timely, relevant, and accurate delivery of information to the decision-maker. The ability to prevail requires the US military to maintain the information advantage and achieve decision dominance over the enemy. The US military can do this by applying information warfare across the spectrum of competition and conflict. Although information warfare has been discussed and debated seriously since the mid-1990s, no universal terms exist in the joint community. Additionally, past US military engagements required robust kinetic capabilities to secure victory. The rise of non-kinetic operations requires an increased focus on operations in the information environment.

The term "information environment" dates to the mid-1990s. During this time, the term focused on the application of Command, Control, Communications, Computers, and Intelligence (C4I) systems. The term most often associated with the information environment at this time was "information dominance." In the 1990s, information dominance focused on information operations, access to intelligence, surveillance and reconnaissance sensors, and space-based asset development.[19] Early United States Air Force (USAF) dialogue focused on creating a mismatch between what, when, and how the US military and its opponent observe, orient, decide, and act. The actor that achieved information dominance would have an advantage in decision-making. Information dominance provided strategic, operational, and tactical advantages across all-domains and provided an opportunity to create a state of paralysis for the enemy.[20]

The 2017 Joint Concept of Operations in the Information Environment (JCOIE) initiated a joint endeavor to deliberately focus efforts on understanding the role of information and information-related activities in securing strategic outcomes and provided the importance of including information into broader operational planning and operational art.[21] This publication

---

[19] Sheila E. Widnall, "The State of the Air Force," *Airpower Journal*, no. IX (Spring 1995): 5.

[20] George J. Stein, "Information Warfare," *Airpower Journal*, no. IX (Spring 1995): 36.

[21] US Department of Defense, Joint Staff, *Joint Concept for Operating in the Information Environment (JCOIE)* (Washington DC: Government Publishing Office, 2018), vii.

provides the current definition of the information environment. Joint doctrine uses the term "information superiority"; however, the term "information advantage" will replace this term in future doctrine updates. The US Army and USAF doctrine notes reflect this change.[22] The US Marine Corps' guidance memorandum, "Definitions for Information Related Terms," does not explicitly reference information advantage; however, it formalizes the terminology and essential elements to achieve information advantage and for conducting operations in the information environment.[23] Furthermore, the term "information dominance" fell out of vogue as it proved to be an unachievable term in military operations.[24]

The term "information warfare" has been defined and redefined since the 1990s. As of June 2020, the US Army and US Navy have not adopted an official definition for information warfare. The definition used in this study is the USAF information warfare definition.[25] All military services have a similar definition for information operations. The joint publication definition of this term is used in this research. Finally, each military service has a similar but different definition of operations in the information environment. This study will use the USAF definition officially published in the June 2020 JADO doctrine annex 3-99.[26] The use of these terms clarifies the discussion and will be used throughout this document when discussing the information environment and denying the enemy decision dominance.

Operations in the information environment represent a significant area for exploitation by the US and its adversaries. Recent global publications articulate concerns over misinformation,[27]

---

[22] US Department of the Air Force, Doctrine Annex, *Annex 3-1 Department of the Air Force Role in Joint All-Domain Operations (JADO*) (Maxwell AFB: Lemay Center for Doctrine, 2020), 6.

[23] Deputy Commandant, Combat Development and Integration, *Definitions for Information Related Terms,* 1-2.

[24] US Air Force, Doctrine Annex, 6.

[25] Ibid.

[26] Ibid.

[27] Claire Wardle and Hossein Derakhshan, *INFORMATION DISORDER: Toward an Interdisciplinary Framework for Research and Policy Making* (Strasbourg: Council of Europe Report DGI, 2017), 20. The following terms are provided for clarity: (1) Misinformation: false information is shared,

disinformation, and malinformation and highlight information disorder's impacts on the decision-maker.[28] In her article "#FakeNews in #NatSec," Amanda Cronkhite discusses how US adversaries seek to control the narrative to shape the American public's perceptions through misinformation and networks.[29] Inaccurate reporting and manipulation of the American people threaten US national security. The distribution of knowledge depends on how it is transmitted. The digital age provides US adversaries additional means in which to broadcast, manipulate, and affect behavior. Understanding that people make choices based on their own interests and values, carefully and intentionally crafted messages aim to target specific audiences. Delivery of these messages is through traditional media publications, social media, and memes. Russia and China actively target the US population and national leaders in the information environment.

Information saturation or "flooding" is another tactic used to disrupt the thinking of a population.[30] As information is repeated, amplified, and spread, the information's accuracy is hard to distinguish and equally challenging to understand the source's origin. Kliman et al. discuss how through astroturfing, the initiator masks his attribution to the original message and links the message to another individual or group within the society allowing the originator to deny his actions. This permits the message to appear more credible than if the audience knew the true origin of the information.[31] While Russian efforts in the information environment aim to

---

but no harm in meant by it; (2) Disinformation: false information is knowingly shared to cause harm; (3) Malinformation: genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.

[28] Ibid.

[29] Amanda B. Cronkhite, Wenshuo Zhang, and Leslie Caughell, "#FakeNews in #NatSec: Handling Misinformation," US Army War College Quarterly Parameters 50, no. 1 (Spring 2020): 6-10.

[30] Daniel Kliman, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche, "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations," Center for New American Security, May 2020, 8, accessed 4 October 2020, https://www.cnas.org/publications/reports/dangerous-synergies.

[31] Ibid., 8-9.

exploit divisions and are generally more confrontational, Chinese actions focus on crafting and delivering a stable narrative that is less visible to the American people.[32]

Information manipulations are also seen in a military context. The Russian Gerasimov Doctrine articulates the ratio of non-military and military action as 4:1.[33] Russia executes targeted military operations in the information environment while intentionally operating under redlines that would initiate armed conflict. Efforts focus on blurring the lines between peace and war, maintaining the competitive advantage, and shaping the environment's political, economic, and social factors. The methods to achieve this involve subversion, espionage, and propaganda. Information conflict, a non-traditional form of warfare, aims to exploit government and military leaders' cognitive processes.[34] These efforts try to reduce the US' coordination and fighting potential.

Reducing overall combat capability requires a new type of warfare. As articulated in the Gerasimov Doctrine, modern warfare (also referred to as Sixth Generation Warfare) includes long-range and precision weapons, simultaneous operations, and reduced time and space for decision-making and action. Creating a unified information space for one's operations while denying the adversary's ability to understand, visualize, lead, direct and assess the situation aims to generate information gaps, disruption, reduce overall decision-making capability, and shape the environment before the opening of hostilities.[35] Russia seeks to achieve an asymmetric advantage through the military's multifarious character acting in the information environment and the operational environment. Effects are maximized through indirect operations with special forces, cyber and information warfare operations, and developing artificial intelligence platforms to

---

[32] Kliman et al., “Dangerous Synergies”, 8-9.

[33] Mary Ellen Connell and Ryan Evans, “Russia’s ‘Ambiguous Warfare’ and Implications for the US Marine Corps,” CNA Analysis and Solutions, 2015, 3-6, assessed on 10 November 2020, https://www.cna.org/cna_files/pdf/dop-2015-u-010447-final.pdf

[34] Ibid.

[35] Gerasimov, “The Value of Science in Prediction,” 2.

rapidly collect, aggregate, and provide actionable intelligence to the warfighter. The Gerasimov Doctrine allows the Russian military to respond to traditional military conflict while simultaneously targeting the opponent's cognitive processes and mind, referred to by some as the sixth domain.[36] Combining these actions allows Russia to deliver low-cost, high-impact effects throughout the competition continuum, achieve asymmetric advantage, and damage the opponent's information systems, resources, and data. Russian actions in the information environment are robust and continuous.

The above discussion highlights the current literature on the topics of the information environment, Reflexive Control, and associated terms. The information environment provides a lucrative space in which an adversary can exploit and manipulate information to shape the target audience's perceptions and attitudes. Such actions can confuse and impact civilian, government, and military decision-making. Invigorating US military planning and operations in the information environment can safeguard vital information for US military and government leaders while simultaneously setting conditions in which the adversary's information can be disrupted, degraded, or manipulated. Information is a new form of firepower. Through non-kinetic, non-traditional means, the US can achieve the information advantage by controlling information systems, processes, and the target audiences. Using a grounded theory methodology, the subsequent sections will explain this study’s theoretical approach, identify common Reflexive Control methods, and develop a proposed US military theoretical approach for operating in the information environment and to achieve decision dominance.

[36] Media Ajir and Bethany Vailliant, “Russian Information Warfare: Implications for Deterrence Theory.” *Strategic Studies Quarterly* (Fall 2018): 70–89.

Methodology

To answer the primary research question, "how might the US deny the enemy decision dominance?" This methodology will employ a Grounded Theory approach. Grounded Theory is a method that systematically evaluates qualitative data to construct a theory from the presented data. Through grounded theory construction, the research question is explored through the sampling of data.[37] In this research, the author will sample several countries impacted by Russian active measures. The data collected from this sampling will be coded, categorized, and analyzed to develop a novel theory. These findings and theories will guide the analytical discussion of this paper.

Russian active measures, or more broadly, its operations in the information environment, provide a repository of publicly available data in which to analyze Russian actions. This research samples five countries: Estonia, Georgia, Ukraine, the Czech Republic, and Lithuania. The sampling of Russian actions in these countries assists in answering the primary research question and provides a more comprehensive understanding of the impact of Russian operations in the information environment as they pertain to future US military actions. The output of this sampling will provide the data necessary to code, assign meaning, and present insight into the analytical connections between events, countries, and Russian actions. The culmination of this research, coding, and analysis drives a new theory – the Theory of Decision Dominance.

Russian Information Warfare and Reflexive Control

Twenty-first century warfare has demonstrated the rise in the hybrid style form of warfare in which asymmetric methods are combined with conventional kinetic and non-kinetic effects to place the opponent at a position of relative disadvantage. The US Joint Force's main

[37] Kathy Charmaz, *Constructing Grounded Theory* (Los Angeles, CA: SAGE Publications Ltd, 2014), 18.

objective is to maintain the advantage across the competition continuum while simultaneously equipping the force to respond across the continuum of armed conflict.[38] With the resurgence of great power competition, Russia and China present a challenge to US interests and national security. Specifically, Russian destructive and aggressive actions within the information environment present a concern to US JADO planning and execution in the future.

JADO is comprised of air, land, maritime, cyberspace, and space domains, as well as the electromagnetic spectrum (EMS). Through the implementation of simultaneous and continuous actions across multiple domains, the speed, effectiveness, and scale with which the US responds can be tailored to gain the advantage and prevail.[39] Underpinning joint force action in the operational environment is the information environment. To ensure domain dominance, it is necessary to understand how our adversary conducts operations in the information environment and to develop a more relevant approach to execute joint all-domain operations. This section will provide an understanding of Russian actions in the information environment by looking at Russian Information Warfare and Reflexive Control. A sampling of Russian operations in Estonia, Georgia, Lithuania, Czech Republic, and Ukraine will demonstrate Russian capabilities and potential implications for US operations in the information environment.

Russian operations in the information environment focus on the idea of information battle or conflict.[40] Operating under the threshold of armed conflict, Russia strives to compete against and influence its adversaries and its populations. Operating in the gray area, Russian actions are continuous, opportunistic, and executed with depth. With careful evaluation of its adversary, Russian measures seek to further divide populations against their governments, propagate discontent, and manipulate the targeted audience. These actions are taken during competition to

[38] US Air Force, Doctrine Annex, 1-19.

[39] Ibid.

[40] Connell and Evans, "Russia's 'Ambiguous Warfare' and Implications for the US Marine Corps," 17.

set the right conditions for the successful application of conventional military force during conflict.[41] The most common active measures in competition include damaging or disrupting information systems, resources, and processes; presenting false or misleading information; attacking the adversary's decision-making at the "filter;" and using lobbyists or non-governmental agencies to propagate its agenda.[42]

Russian active measures are part of a national-level information warfare strategy. Russian information warfare activities demonstrate an integrated and interdisciplinary approach to understanding and analyzing its adversaries.[43] Information is part of Russian foreign policy and is an integral part of Russia's layered, whole of government approach to target and weaken its opponent.[44] Information is a weapon; a weapon with unlimited range and significantly less expensive than highly advanced kinetic weapons.[45] As part of Russia's new-generation warfare (the US term for Reflexive Control and the Gerasimov Doctrine), leveraging offensive information warfare measures allows Russia to create inter-state competition space in which the "battlespace" is no longer linear or fixed. Information warfare activities stretch beyond traditional state boundaries, are conducted on a continuous basis and without a formal declaration of war.[46] With the rise of the Information Age, Russia continues to expand its information warfare capabilities and challenge existing paradigms of peace and war through the weaponization of information.

---

[41] Gerasimov, "The Value of Science in Prediction," 2-3.

[42] Ion Mihai Pacepa and Ronald J. Rychlak. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism* (Washington, DC: WND Books, 2013), 38-41.

[43] Kevin N. McCauley, *Russian Influence Campaigns Against the West: From the Cold War to Putin* (South Carolina: CreateSpace Independent Publishing Platform, 2016), 341.

[44] Can Kasapoglu. "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," *National Defense College*, no 121 (2015), 6.

[45] Schultz and Godson, *Dezinformatsia*, 13; Thomas. *Recasting the Red Star*, 245.

[46] McCauley, *Russian Influence Campaigns Against the Wes*t, 343.

Using information as a weapon, Russia seeks to undermine democracy and democratic values, weaken the cohesion of the US, its allies and its partners, and reduce US global influence while increasing Russian prestige on the world stage.[47] Deliberate and strategic information warfare activities allow Russia to legitimize its power and deny forcible action. Russia's strategic efforts allow them the opportunity to control the information space, manipulate various audiences, propagate discontent, and provide legal cause for its aggressive actions. As an instrument of national policy and a vital component of its foreign policy, Russia seeks to achieve dominance and control with minimal physical confrontation.

Russia's information warfare strategy provides the opportunity to execute continuous offensive operations during peacetime that have debilitating impacts on its adversaries while also controlling escalation and minimizing armed conflict.[48] Maintaining escalation control and limiting military action requires the deep targeting of the opponent's cognitive processes and information systems. Russian information warfare strategy has two components: information-psychological and information-technical.[49] Information-psychological, executed through information operations, focuses on deconstructing the situation and narrative.[50] Russian actions sow discontent by exploiting fissures and further polarizing the targeted audiences. Russian misinformation, disinformation, and malinformation operations create confusion, distrust, and shape public perceptions that benefit the interests of the Russian government.[51] Agents carefully craft and manipulate messages, disseminate them through multiple media and social platforms, and aggressively amplify the message to the target audience. Through astroturfing and flooding, Russian information operations strive to influence the decision-making cycle of the adversary

[47] Kliman et al., "Dangerous Synergies", *20.*

[48] Ajir and Vailliant, "Russian Information Warfare," 70–89.

[49] Thomas, "Russia's Reflexive Control Theory and the Military," 308.

[50] Kliman et al., "Dangerous Synergies", 10.

[51] Wardle and Hossein, *INFORMATION DISORDER*, 20-22.

without their conscious understanding of the action being taken against them.[52] Continuous and robust information-psychological activities influence a population and allow Russia to achieve a level of information advantage at a lower cost and with high operational impact.[53]

Achieving information advantage requires adequately targeting the adversary's cognitive filter. A cognitive filter is the way in which one separates necessary information from useless or irrelevant information, and is based on one's understanding of the operational environment, subject matter knowledge, information resources, and personal experience.[54] The filter is the collective image of one's methods and techniques for organizing and processing information for action. It is a psychological depiction of a person's cognitive processes as well as the associated information processing systems and resources in use.[55] Through information-technology methods, Russia targets the hardware and software resources, processes, and systems of its adversary.[56] By targeting these resources, processes, and systems, decision-making is altered to generate a specified behavior or desired action. Information-technology focuses on cyber warfare means to include cyber network operations, deception, and electronic warfare. The aim is to disrupt the system's processes, data access and retrieval, or provide opportunities to gain unauthorized access.[57] By controlling the filter, Russian actions degrade the availability of information, manipulate data to shape perceptions, and alter the integrity of the system. These actions allow Russia to control decisions, damage intelligence apparatuses, and model the reasoning of its opponent.[58] The combination of information-psychological and information-

[52] Wardle and Hossein, *INFORMATION DISORDER*, 20-28.

[53] Ibid., 28; Ajir and Vailliant. "Russian Information Warfare," 70–89.

[54] Thomas, "Russia's Reflexive Control Theory and the Military," 243.

[55] Ibid.

[56] Ibid., 138.

[57] Ibid., 247-249.

[58] Kasapoglu, "Russia's Renewed Military Thinking," 4.

technology concepts establishes the framework for Russia's information warfare strategy and the achievement of broader national objectives.

Foundational to Russia's information warfare strategy is the theory of Reflexive Control. More specifically, Reflexive Control theory is an information warfare means in which the actor aims to convey deliberately prepared information that coerces the targeted audience into making a decision desired by the originator.[59] Reflexive control theory seeks to control the narrative, influence the target audiences' actions, and shape perceptions, attitudes, and behaviors of decision-makers. This requires an understanding of the adversary's patterns of behavior, historical decision-making and processes, and the systems he uses to communicate and aggregate information.[60] The focus of Reflexive Control is the intersection between mental and information processes (the filter) and psychological impacts of information related to the adversary's assessment of the situation and available response options.[61] The ability to exploit and control the adversary's decision making calculus and deny him decision dominance requires the actor to visualize the adversary's anticipated patterns and actions.[62]

Reflexive Control theory has two parts: reflection and control.[63] Reflection is the art and science of understanding how the adversary thinks and acts. This requires a firm understanding of the politics, ideology, military doctrine, tactics, and capabilities, political and military objectives, and overall strengths and weaknesses of the targeted organization. Using this knowledge, reflex is the specific process of modeling the reasoning or behavior of the adversary with the goal of

---

[59] Thomas, "Russia's Reflexive Control Theory and the Military," 241.

[60] S. Leonenko, "Refleksivnoe upravlenie protivnikom" [Reflexive Control of the Enemy], *Armeiskii sbornik [Army Collection]*, no. 8 (1995): 28, quoted in Thomas, "Russia's Reflexive Control Theory and the Military," 241.

[61] Kasapoglu, "Russia's Renewed Military Thinking," 5.

[62] McCauley, *Russian Influence Campaigns Against the West*, 14, 327.

[63] Ibid., 14.

altering his decision making in a disadvantageous way to him.[64] Control involves altering the adversary's decision-making process without him knowing or understanding that his decisions are being influenced from an outside source. The goal of Reflexive Control is to shape the information environment by providing more predictability and control of the situation to the individual using the theory.[65]

Shaping the information environment and maintaining control of the situation is enabled through knowing the adversary's collection and analytical processes, goals, and decision-making processes. Understanding these elements allows for the transfer and control of specific information to the adversary. Transferring and controlling the information presented to the adversary can take four forms: power pressure; measures to present false information; influencing the decision maker's processes; and by altering the decision maker's time.[66] The power pressure method involves using superior force, demonstrating force through actions like shows of force or shows of presence, or through ultimatums.[67]

The second form, presenting false information, focuses on the Russian term *maskirovka* translated to mean deception and denial.[68] Measures to present false information include misinformation or disinformation, distortion of information and concealment.[69] These measures deny the adversary the ability to understand the ground truth in the information and operational environments, mislead his actions, and create hesitation in his decision-making. A key component requires ensuring that the information presented appears plausible and represents what the

[64] Thomas, "Russia's Reflexive Control Theory and the Military," 241.

[65] McCauley, *Russian Influence Campaigns Against the West*, 9.

[66] Thomas, *Recasting the Red Star*, 127.

[67] Ibid., 126.

[68] Connell and Evans, "Russia's 'Ambiguous Warfare' and Implications for the US Marine Corps," 3.

[69] Thomas, *Recasting the Red Star*, 126.

adversary understands as true in the environment.[70] Thirdly, information can be transferred and controlled by influencing decision-making algorithms.[71] Methods include creating conditions for "normal" exercises, deliberately presenting and executing false doctrine, or using different modes and codes than operationally listed to confuse or mislead the adversary of one's true intent. The fourth method for transferring and controlling information involves altering the decision maker's time in which actions are taken. Action can include forcing an operation to commence earlier than planned or causing the adversary to make a quick (yet unnecessary) decision.[72] The multi-disciplinary methods of transferring knowledge to the adversary shape the information and operational environments and maintain control.

By creating a well-controlled and unified information space, it is possible to achieve decision dominance and hinder the adversary's ability to develop the situation and respond appropriately.[73] Through Reflexive Control theory, the adversary's cognitive functions, reasoning, and behaviors are replicated and generate effects by targeting his cognitive and information processing filters. Denying the availability of information, altering information, or injecting misleading information at the filter creates a condition in which the adversary makes a decision he thinks is well-reasoned and beneficial to his situation but is actually the initiator's desired outcome.[74] The application of this theory results in the ability to influence the adversary's combat plans, formations, force posturing actions, and his perception of the situation.

[70] McCauley, *Russian Influence Campaigns Against the West*, 18.

[71] Thomas, *Recasting the Red Star*, 126.

[72] Ibid., 127.

[73] Gerasimov, "The Value of Science in Prediction," 2.

[74] Schultz and Godson, *Dezinformatsia*, 38.

Russian Operations in the Information Environment

Russia's information warfare strategy and use of Reflexive Control is not a new concept. However, the rapid growth and development of the Information Age makes these efforts more impactful as traditional armed conflict declines and a persistent state of competition prevails. Since the mid-2000s, Russian operations in the information environment remain focused on destabilizing NATO members, sending threatening messages to former Soviet Union Republics, and undermining US influence and action regionally and on a world stage.

In 2007, Russia demonstrated the ability to initiate and control the crisis in Estonia through a combination of well-placed information warfare capabilities. Through the influence of a local indigenous Russian population, and a mix of psychological, economic, cyber, and cultural measures, Russia intimidated and internally disrupted Estonia.[75] Russian measures included a robust propaganda and information operations campaign against the Estonian government. Information operations messages declared the government fascist and oppressive to ethnic Russians in the country and region.[76] Russia fueled demonstrations inside of Estonia. Attempting to provoke violence and forcing the Estonian government to respond, Russia established a specific and legal reason to intervene on behalf of their citizens.[77] Further analysis shows that Russian special operations forces, dressed in civilian clothes, moved swiftly into the country to accelerate, and instigate the violence. Aggressive cyber-attacks on government and banking sectors targeted mission-essential computers. Persistent distributed denial of service (DDoS) attacks hindered information flow and control. These non-kinetic measures created wide-scale confusion, undermined the government's influence, and demonstrated Russian influence and power over a NATO country. Through limited physical means, Russia sent a clear internal

[75] McCauley, *Russian Influence Campaigns Against the West*, 387.

[76] Ibid., 384.

[77] Ibid., 383-386.

message to Estonia that the NATO alliance was not capable of halting Russian influence and action in its country, and an external message that other Baltic State countries remained vulnerable to Russian influence and control.

Russia further demonstrated information warfare methods in Georgia in 2008. Through a calculated plan, Russia created close economic and bureaucratic ties with Abkhazia and South Ossetia and carefully crafted and resourced military action.[78] The Russian objectives included: sowing fear and confusion in the Georgian government, determining Western response, and setting military conditions. Russia built rapport and legalized action by issuing passports to the citizens of Abkhazia and South Ossetia. Through time, and under the guise of its peacekeeping mission, Russia established a de facto annexation. In April 2008, Russia increased its peacekeeping troops in Abkhazia to more than 500.[79] Under the pretense of railroad repairs, Russia's increased presence allowed for the clandestine movement of equipment and special forces, disguised in civilian attire, into the region. Additionally, Russia executed Exercise Kavkaz (Causus) '08, in which large numbers of troops were placed on the border.[80] Preparation for this exercise provided a routine reason for increased transport movement, and military equipment and troop deployment along the border between Russia and Georgia. Additionally, Russia desensitized the Georgian response in the year leading up to the invasion through repeated air incursions with fighter aircraft.[81] Through calculated action, Russia normalized the situation and messaged its non-hostile intent in the region and to NATO.

In early 2008, Russia ratcheted up its political and diplomatic pressure on the capital of Tbilisi. It aimed to sever relations between key leaders and cause confusion within the

[78] Ariel Cohen and Robert E. Hamilton, “The Russian Military and the Georgia War: Lessons and Implications” (US Army War College, 2011), 6, accessed 13 September 2020, www.jstor.com/stable/resrep11808 JSTOR.

[79] Ibid., 6.

[80] Ibid., 19.

[81] Ibid., 21.

government.[82] Additionally, routine military action served to complicate the decision calculus of the US and NATO and how they should respond to Russian action in the region and against Georgia.[83] When Russia initiated physical action to secure Abkhazia and South Ossetia, cyber operations supported military action. Cyber efforts targeted 38 Georgian and Western websites, the Georgian President and Minister of Foreign Affairs, the country's Supreme Court, and the embassies of the US and the United Kingdom. Forensic analysis reveals that these actions were under central direction and control by a Russian proxy agent.[84] Information operations, propaganda, and disinformation signaled that Russia initiated offensive action against Georgia after aggressive actions were taken against its peacekeepers. The Russian information narrative, broadcast across multiple media channels, networks and press conferences, emphasized the legal nature of Russia's intervention to protect its citizens and to provide humanitarian aid. Russia was the victim and not the aggressor.[85]Russian actions in Georgia demonstrate how ambiguous military action and peacekeeping operations can complicate and confuse decision-making and awareness of the situation. Russia aimed to exploit political tensions and fissures and to provide plausible deniability for its increased military force posture. Through this layered and complex network of information warfare activities, Russia achieved significant success with minimal physical military engagement.

The 2014 annexation of Crimea represents one of the most significant and sophisticated actions undertaken by Russia in recent history. Through deliberate and well-planned operations, Russia executed cyber, electronic warfare, and information operations activities to achieve political aims and to complement its tactical level military actions. Cyber operations targeted mobile networks, internet and wireless networks, and more robust command and control

[82] Ibid., 18.

[83] Kasapoglu, "Russia's Renewed Military Thinking, 9 -10.

[84] Cohen and Hamilton, "The Russian Military and the Georgia War," 44.

[85] Ibid., 47.

infrastructure. Ukrainian military command and control, and individual soldier communications proved ineffective and highly targetable.[86] Russian forces used publicly acquired information and signals intelligence to understand and influence Ukrainian action and decision-making. Propaganda and information operations hardened the resolve against Ukrainian forces and the government, the West, and NATO.[87] Compromised telecommunication networks allowed Russia to interrupt and broadcast specifically tailored information at the filter across Ukrainian and Western internet sources.[88] Russian agents sent malicious and threatening texts to Ukrainian soldiers and their families, flooded the information space, and built out contact lists for further targeting. Through what is referred to as "man-in-the-middle" attacks, Russia manipulated protocols in the information environment and sent misleading orders and information to the soldiers on the ground.[89] DDoS attacks created confusion and delayed communication between the government, the military, and its people. Additionally, Russian agents manipulated information and generated harassing attacks to undermine the government.[90] The outcome resulted in a demoralized and confused military with an increased sense of uncertainty about the information and operational environments.

Furthermore, Russian propaganda and disinformation efforts proved robust in Ukraine. Russia built a "big lie" in which it successfully presented an alternative reality built on a "kernel of truth."[91] Advanced sensors and other reporting mechanisms identified the Russian movement, yet this information was not taken as fact. News agencies failed to understand the ways in which

---

[86] Aaron F. Brantly, Nerea M. Cal, and Devlin P. Winkelstein, "Defending the Borderland: Ukraine Military Experiences with IO, Cyber and EW," Army Cyber Institute at West Point, 2017, 25, accessed 10 November 2020, https://cyberdefensereview.army.mil/Portals/6/Documents/UA%20Report%20Final%20AB.pdf.

[87] McCauley, *Russian Influence Campaigns Against the West*, 383-386.

[88] Brantly, Cal, and Winkelstein, "Defending the Borderland," 36.

[89] Ibid.

[90] McCauley, *Russian Influence Campaigns Against the West*, 412.

[91] Pacepa and Rychlak, *Disinformation*,38-41.

Moscow manipulated reporting. The Kremlin flooded the information environment and hindered understanding through repetitive contradictions and denial of action messages.[92] Agents manipulated videos and photos to support the information message as well as used "role players" to present a specific narrative about the "atrocities" on the ground.[93] The combination of these actions created uncertainty, delayed decision-making, and undermined the legitimate authority's ability to control the situation within its borders. The outcome resulted in Russia's ability to shape the battlespace and information space to its advantage.

Russian information warfare activities continue today. Less is known about the persistent and continuous actions to undermine democracy, propagate discontent, and damage the influence of NATO and Western nations in the Czech Republic and Lithuania. In the Czech Republic, Russia continues to take advantage of discourse and weaknesses between the government and their people with the ultimate objective to confuse or shift public opinion towards supporting initiatives and policies of Moscow.[94] Through disinformation and amplification, conspiracy theories, and propaganda, Russia creates a unified information space with a strong narrative supporting Russian objectives.[95] In 2013, various sources attributed Russia with broadcasting the "Juvenile Justice" video on YouTube. The message in this video accused France, Germany, and Nordic countries of tyranny against the Czech Republic and the parties responsible for the abduction of their children. [96] Similar disinformation campaigns aim to influence anti-US sentiment and to convey overly aggressive US actions and interference to control and influence the Czech Republic. Anti-Western propaganda carries the repetitive message that the US is

[92] Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War*, Report 1 (2015), 13.

[93] Ibid.

[94] McCauley, *Russian Influence Campaigns Against the West*, 437.

[95] Albin Sybera, "Truth Missing in Action in Czech Information Wars," *Balkan Insight* (Sarajevo: 2019), accessed 11 December 2020, https://balkaninsight.com/2019/09/09/truth-missing-in-action-in-czech-information-wars/.

[96] Ibid.

planning to control the world, influence Czech leaders, government, and people, and actively trains and supports agents to undermine the Czech Republic's interests.[97] This same information narrative conveys the moral, economic, and political corruption of the US and the West. Disinformation messages are repeated, or amplified through social media, public events, the Russian embassy, and Russian media outlets broadcasting in the Czech Republic. Russia maintains plausible deniability for these actions by stating that the agents of disinformation do not maintain an allegiance or affiliation with Moscow.[98]

Russian political and military actions in Lithuania maintain a large focus on propaganda and disinformation operations. The Russian embassy in Lithuania generates and distributes propaganda within the country. Information operations and associated messages are delivered through cable television, Facebook, and statelets with a common theme of challenging Lithuania's history and right to exist, while supporting Russian language, culture, and history within the country.[99] Russian sponsored sporting and other social events are used to reach broader populations and to extend the reach of the Russian information operations and influence.[100] Through cultural events, television and radio broadcasts, and a large ethnic Russian population in country, Russia continues to expand its influence and undermine Lithuanian national identity.[101] Russian military units exercise on the Lithuanian border on a recurring basis. These actions create

---

[97] Adela Kleckova, "Russia Targeting the Czech Republic over Statue Calls for International Reaction" The German Marshall Fund of the United States, 2020, accessed 21 October 2020, https://www.gmfus.org/sites/default/files/Russia%20Targeting%20the%20Czech%20Republic%20over%20Statue%20Calls%20for%20International%20Reaction.pdf.

[98] Sybera, "Truth Missing in Action in Czech Information Wars."

[99] Christopher Woody, "Baltic States Think Russia Is Laying the Groundwork for Looking 'Kinetic Operations," *Business Insider*, April 3, 2017, accessed 21 October 2020, https://www.businessinsider.com/russia-propaganda-in-lithuania-attack-on-the-baltics-2017-4.; and McCauley, *Russian Influence Campaigns Against the West*, 440.

[100] Linas Jegelevicius, "In Lithuania, Russia's War for Influence Is Waged with Cable TV and Basketball," *EuroNews*, October 13, 2020, accessed 21 October 2020, https://www.euronews.com/2020/10/13/in-lithuania-russia-s-war-for-influence-is-waged-with-cable-tv-and-basketball.

[101] McCauley, *Russian Influence Campaigns Against the West*, 441.

ambiguity of Russian intent while providing Russia opportunities to swiftly act against the country of Lithuania if it chooses to do so.[102] Force posturing and ambiguity create an environment in which the government of Lithuania and its allies might have difficulty responding quickly to aggressive action. Russia also maintains close ties and affiliations with two political parties, the Russian Alliance and Electoral Action of Poles, which allows them access and influence to Lithuanian government decisions and policies.[103] Finally, like it does in other former Soviet Union Republics, Russia maintains the right to represent and defend the interests of the ethnic Russians living within the country. Russia's persistent information warfare actions allow it to shape the information environment, influence large populations, and set conditions that are favorable to Russian political and military objectives in the future.

As one can see from the sampling above, Russian information warfare operations are robust, well embedded within societies, and are built to extend Russian influence and control. While Russian information warfare capabilities vary based on the environment, political aim, and country, several themes become apparent. Based on the research findings, Russia most effectively employs its information warfare strategy through the active measures of damaging and disrupting information systems, presenting misinformation and disinformation, attempting to influence and disrupt the adversary's filter, and through economic and cultural means. Understanding how and when Russia determines to use these measures will help the US military and civilian planners shape, influence, and control operations in the information environment.

Analysis

Competition for information is not a novel concept. The Information Age and developments in information technology and information systems create greater and more

[102] Woody, “Baltic States Think Russia Is Laying the Groundwork for Looking ‘Kinetic Operations."

[103] Woody, “Baltic States Think Russia Is Laying the Groundwork for Looking ‘Kinetic Operations."

significant opportunities in the information environment. Information warfare is a means to accomplish the mission of the USAF. JADO requires widespread integration of information systems and information capabilities into joint operations. Rapid and reliable transmission, analysis, and exploitation of information underpins the military's ability to effectively attack, defend, and exploit the adversary. Information as a function enables the pinpointed delivery of advanced weapons and provides the opportunity to manipulate or deny access of information to the adversary. Information provides vital resources to US decision-makers while simultaneously acting as a product, potential target, or potent weapon to diminish the adversary's combat capability. Information warfare is a key function to integrate warfighting disciplines and to target an adversary's physical behavior and cognitive decision-making processes more effectively. Operations in the information environment require deliberate thought at the start of planning and must continue throughout the course of an operation until national objectives are achieved.

Beginning in 1997, the USAF identified the need to develop information warfare procedures and doctrine to better organize, train, equip, and employ its military forces.[104] Recent information related technological developments allow access and transmission of high-quality data at unprecedented rates. As first identified in 1997, "the commander with the advantage in observing the battlespace, analyzing events, and distributing information possesses a powerful, if not decisive, lever over the adversary."[105] Modern developments provide the opportunity to gain direct access to the adversary's information, information systems, and intelligence apparatuses. Information can be altered or created more easily. Information warfare measures – information operations, electronic warfare, cyber operations and intelligence, surveillance, and reconnaissance – can be used to attack, defend, or exploit the adversary's resources, capabilities, and information. Measures taken in the information environment enable more effective operations overall.

---

[104] Sheila E. Widnall and Ronald R. Fogleman, *Cornerstones of Information Warfare.* (Washington, DC: Department of the Air Force, April 1997), 1-4.

[105] Ibid.

The USAF Command and Control in the Information Environment (C2OIE) concept builds upon the initial ideas discussed in the 1990s and joint concepts like the JCOIE. Efforts focus on how to place information at the "forefront of operational-level planning, execution, and assessment."[106] In order to expand the competitive space with allies and partners, diminish the adversary's competitive space, and deny freedom of action in the information and operations environments, information must be integrated at the forefront of planning.[107] JADO planning and execution in competition and in conflict requires the ability to expose malign influence, weaken the competitor's alliances through focused messaging, and deceiving or manipulating the adversary's decision-making.[108] This can be accomplished through altering, disrupting, and destroying information and information systems used by the adversary. The goal of these actions is to reduce the adversary's ability to sense, observe, orient, understand, respond, and make advantageous decisions when faced with multiple dilemmas.

With the USAF's focus on information warfare, Russian information warfare and Reflexive Control methods provide valuable insight into controlling, exploiting, and enhancing information to bolster US operations and to deny the adversary decision dominance. Based on the sampling of Russian operations in the information environment in Estonia, Georgia, Ukraine, the Czech Republic, and Lithuania, several themes emerge to help define Russia's strategy: a whole-of-government approach, execution of information warfare activities (to include Reflexive Control theory and associated methods), and the concepts of information conflict and information firepower (see Table 1, page 48). The combination of these factors enables Russia to maintain the information advantage and to achieve decision dominance through damaging and disrupting

[106] Sandeep S. Mulgund and Mark D. Kelly, *Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment* (Washington, DC, HAF A3, September 2020), 4.

[107] Mulgund and Kelly, *Command and Control of Operations in the Information Environment in Operational Planning*, 3.

[108] Ibid.

information systems, presenting misinformation and disinformation, and by attempting to influence and disrupt the adversary's filter.

Using a whole-of-government approach Russian information warfare methods exploit the gray zone between peace and wartime declarations while maintaining inter-state competition. Active measures are continuous and seek to find opportunities to legitimize and legalize Russian action and power. These actions are deliberate, planned, and calculated to minimize escalation and shift the worldview from the US and Western powers to a Russian focused world. Russian Reflexive Control is the primary means that enables its information warfare strategy. Russia continuously acquires, processes, exploits, and disseminates information to deceive, influence, and manipulate the targeted audience. Efforts focus on information systems and cognitive processes used by the adversary. Russia uses robust Reflexive Control tools to identify, deconstruct, and target an adversary's cognitive filter. This is done through disrupting how the target senses, understands, and processes information in his environment. By carefully modeling the reasoning of its adversary, Russia attempts to alter the perceptions and the actions taken by its opponent. In this sense, information is a weapon that weakens authority, creates fissures in populations, alters analytical findings, creates fog and friction in the information and operational environments, and seeks to damage and disrupt the information systems and processes. The goal is to change the behavior of the decision-maker.

Through the weaponization of information, Russia demonstrates the importance of information conflict. Through its non-lethal or non-kinetic measures, such as discrediting sources, influence operations, and propagating discontent, Russia wields control and bolsters its inter-state competition. Actions in the information environment have global reach and flexibility, and are persistent. Russia manipulates information to achieve a relative advantage in competition. This provides Russia the opportunity to reduce the rise to armed conflict and nullifies the lethality of traditional military weapons. Russia focuses on information as the linchpin to its all-domain and hybrid operations. This allows it to target the adversary's information resources, systems, and

filters with the goal of reducing decision dominance and effective combat generation of the adversary. Lastly, information is a form of firepower. Information is used by all societies across the world. Through Reflexive Control methods and information warfare techniques, Russia uses information to target populations, militaries, and decision-makers. These measures aim to achieve results and preserve Russian freedom of action by preserving time and space for Russian military and political action, when necessary. Well placed information or the ability to deny information to a targeted audience allows Russia to corrupt, degrade, and negatively impact the adversary's ability to command and control and make smart decisions about the situation. It is through these measures – whole-of-government, information warfare (to include Reflexive Control), information as conflict, and information as the new form of firepower – that Russia has successfully unified the information space and reduced the combat capacity of its adversaries in recent conflicts. These findings are supported by the sampling of Russian operations in the information environment discussed above.

Understanding the way in which an adversary operates in the information environment is imperative for future US military action. It is essential that the Joint Force develop an integrated and robust strategy leveraging information warfare capabilities and outcomes to deny the adversary the ability to freely operate in time and space. Given the primary research question, "how might the US deny the enemy decision dominance?" the following theory – Decision Dominance Theory – is presented. This theory seeks to provide a way to deliberately use information to target an adversary's behavior and information systems. The goal is to deny the adversary the ability to perceive and recognize the situation and hinder his ability to effectively use the information presented to him to make calculated decisions. The above research and understanding of Reflexive Control theory shaped the development of this theory.

Decision Dominance Theory:

Decision dominance is achieved through informational power, which is secured by controlling information, exploiting information, and enhancing information to one's benefit. Informational power can achieve the same effect, or greater effect, as physical firepower. It enhances joint all-domain military power and effectiveness by anticipating an adversary action, understanding an adversary's motives, managing and manipulating information, altering decision algorithms, and developing opportunities, activities, and investments (OAI)[109] in the information environment.

- **Decision Dominance:** a desired state in which commanders sense, understand, decide, and act faster and more effectively than their adversaries.[110] Decision Dominance works within the enemy's decision-making cycle to remove the sanctuary of time and to eliminate options in space.
- **Informational Power** is the ability to leverage information to shape perceptions, attitudes, and other elements that drive desired behavior and the course of events. Informational power involves the ability to acquire, process, distribute, and employ data to maximize combat power.[111] The author further asserts that informational power is achieved through the *control, exploitation, and enhancement* of *information* which allows for persistent, flexible, and well-calculated information warfare outcomes to bolster combat power and deny the enemy decision dominance (see footnote).[112]

[109] Mulgund and Kelly, *Command and Control of Operations in the Information Environment in Operational Planning*, 3. Operations, Activities, and Investments (OAIs) can be overt, covert, or clandestine actions take to shape the operating environment across the competition continuum. The results of OAIs are used to refined strategic approaches.

[110] US Army Cyber Center of Excellence, *Information Advantage*, 3.

[111] US Joint Staff, *JCOIE*, 15.

[112] Note: This definition is an expansive of the JCOIE definition for “informational power” listed in the introduction of this paper. The author has elaborated on this definition to provide clarity on the term and method to achieve informational power.

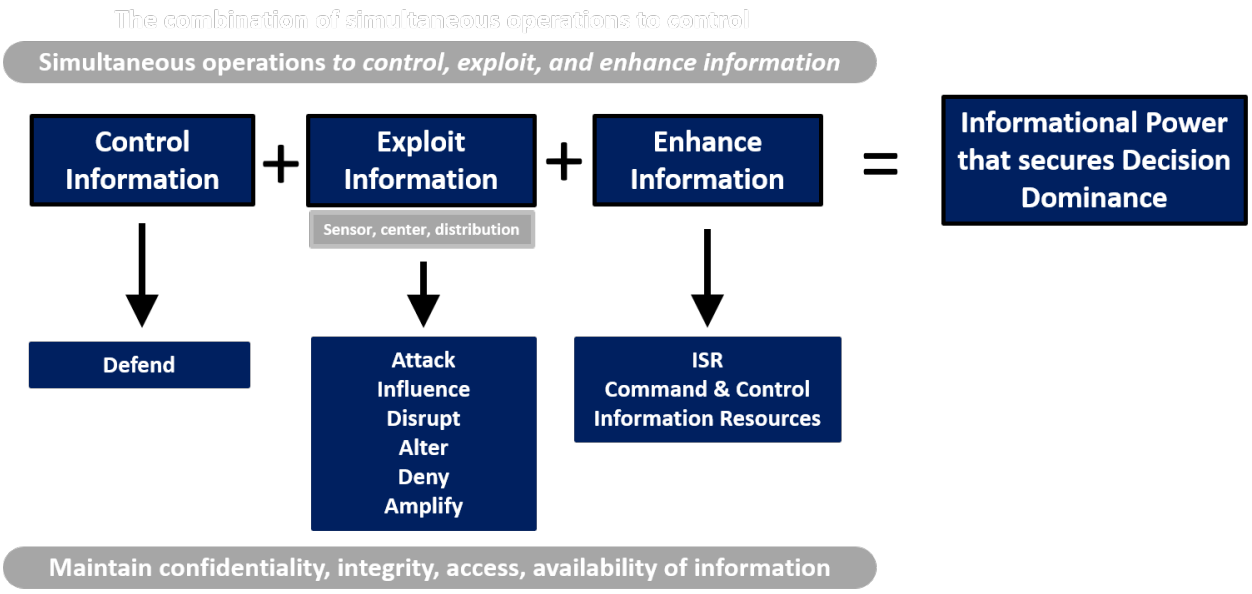

Figure 1. Decision Dominance Theory. Created by author.

Informational power – the combination of *controlling information, exploiting information, and enhancing information* – will allow the US to integrate operations in the information environment into JADO planning and execution. This will enable planners to use information to effect outcomes. Information warfare capabilities – information operations; electronic warfare; cyber; and intelligence, surveillance, and reconnaissance (ISR) – provide the means to alter an adversary's command and control processes, reduce decision-making, and diminish the effectiveness of his combat operations. Combined, informational power and physical power will reduce the combat effectiveness of the adversary by creating multiple dilemmas in the environment that cause confusion and delay or deny the enemy's ability to act appropriately. The combination of informational power and physical power strengthens military power.

The first pillar of informational power, *controlling information*, involves protecting one's own networks against enemy disruption or manipulation. Maintaining the control of information transmission and information systems ensures the confidentiality of the information, the integrity of the information, and the availability of the information to US planners and operational units. Uninhibited access to trustworthy systems and associated architecture ensures the most timely and relevant information guides decision making. Denying the control of information to the adversary prevents him from understanding his environment, creates uncertainty, and complicates his decision-making.

Decision-making is also impacted by the *exploitation of information*. Exploitation, the action of making use of and benefiting from resources, involves altering, changing, or manipulating information to one's benefit. This is most effectively done through understanding of the adversary's information and cognitive filters, information systems, and intelligence architecture. The ability to create an information warfare outcome is contingent on the ability to carefully craft information and place it at the right time and place in the enemy's decision-making cycle. Information can be targeted or weaponized at four filter points – the sensor, the analytical center, the distribution point, or the individual.[114] Using the filter, one can degrade the collection and quality of the information available to the decision-maker, resulting in an incomplete or

[113] US Joint Staff, *JCOIE*, 15. Figure 2 builds on the conceptual ideas listed in JCOIE. Military Power is an instrument of national power. Figure 2 and associated text asserts that informational power is equal to physical power. The combination of informational and physical power maximizes military power.

[114] Jeremiah Deibler, "Winning Wars of Cognition: Posturing the Air Force for the Tactical Information Fight," accessed 13 September 2020, https://othjournal.com/2020/02/10/winning-wars-of-cognition-posturing-the-air-force-for-the-tactical-information-fight/.

intentionally misrepresented understanding of the situation. Decisions are made and specific actions are taken based on the perceived understanding of the environment. The ability to interdict information flow prevents and delays essential data from reaching the organization and results in a decreased ability to sense, understand, and develop the situation. Traditional information operations activities combined with deliberate and persistent targeting at the adversary's filter will enable opportunities to simultaneously target the agent, the message, and the interpretation of the presented information. In turn, this can slow the adversary's ability to sense, observe, orient, decide, and act, promote a mistaken conclusion, and corrupt decision-making capability.

Enhancing information allows one to develop strategic objectives and options that create multiple dilemmas for the adversary across time and space.[115] This requires robust, agile, and layered ISR resources and integrated command and control processes. JADO planning and execution requires the ability to maneuver at tactical, operational, and strategic echelons simultaneously, across all-domains, and with a unified information space. Coordinated planning requires an understanding of the situation, the ability to observe patterns and behaviors, and identify changes in the information and operational environments. Underpinning one's ability to enhance information is trust. Trust encompasses the weight that the group or individual assigns to the integrity of the collected information.[116] Information that is processed, filtered, and analyzed in context answers a specific gap in knowledge. This processed information is known as intelligence. Armed with accurate intelligence and well-understood assumptions, the decision-maker can more accurately assess the situation, shape the environment, and degrade the adversary's own decision-making processes. In this way – information, more specifically

[115] US Department of Defense, Joint Staff, *Joint Doctrine Note 1-19: Competition Continuum* (Washington, DC: Government Publishing Office, 2019). Note: Joint Doctrine Note 1-19 defines "enhance" as "Achieve strategic objectives, prevent the competitor from achieving incompatible objectives, and improve relative strategic or military advantage without causing an escalation to armed conflict."

[116] Ibid.

enhanced information (or intelligence) – is a weapon that can be used to manipulate and deceive an adversary and deprive him of the ability to make decisions that are in his best interests.

The combination of *controlling, exploiting, and enhancing information* allows the decision-maker to have informational power. Informational power enables the information advantage which, in turn, secures decision dominance. The ability to enhance information allows one to observe an enemy's habits and behaviors, helps one to understand the enemy's motives and intent, and locate the enemy's combat capability. Managing, amplifying, and manipulating information allows targeted and well-crafted messages to reach the designated audience. Misinformation and disinformation that resembles past messaging can target the enemy at the filter. Messages that enter an intelligence apparatus at the filter of the information system target the sensor, the analytical center, and the distribution of information to the warfighter. Additionally, through presenting false or misleading information at a perceived credible source, the decision-making algorithm of the enemy can be altered. Presenting specific information at a specific time and place can change the understanding of the environment and alter behavior. This can also cause one to alter his time horizon. With increased uncertainty, one might choose to accelerate or decelerate his plan based on the perceived situation.

While each part of this theory, taken separately, does not present anything novel, two things are significantly different. First, information must be considered at the forefront of military planning and be integrated with traditional physical power. The military culture assumes that physical power is supreme. Modern war demands that informational and physical power be considered on an equal level. Second, activities to *control, exploit, and enhance information* are functions embraced by the USAF now; however, cross-domain and cross-functional integrated planning is limited. The missing link is the intentional integration and dedicated process to incorporate the available capabilities across all-domains in a synchronized and deliberate process. To achieve decision dominance and gain the information advantage through informational power, operations in the information environment must be incorporated into the planning processes like

the Joint Planning Process (JPP), the Military Decision Making Process (MDMP), the Marine Corps Planning Process (MCPP) and the Joint Operational Planning Process for Air (JOPPA). Command and Control must adequately account for non-kinetic and kinetic actions across all-domains – air, space, cyber, land, and maritime. The ability to execute operations in the information environment requires a centralized planning process at the operational level to simultaneously plan and execute control, exploitation, and enhancement of information. This does not currently exist. Centralized planning will enable an integrated approach that can be joined with physical firepower. Control protects US networks and plans while denying the enemy access to vital information. Exploitation allows the opportunity to deny, degrade, disrupt, alter, and amplify information used by the adversary. Enhancement provides key ISR collection required for decision-making, targeting, and tactical action in the environment. Informational power provides the commander with the opportunity to effectively process, analyze, and act on data and information while denying the same ability to his opponent. Therefore, achieving decision dominance requires a coordinated and synchronized plan that leverages control, exploitation, and enhancement of information across all-domains and warfighting functions with the goal of unifying the information space.

Recommendations

This paper articulates the importance of unifying the information space to achieve decision dominance through well-planned and integrated operations in the information environment. The ability to execute joint all-domain operations adequately requires a renewed emphasis on information and information warfare activities in the planning cycle. This study makes four recommendations:

Recommendation 1: The Joint Force should consider the requirements to achieve informational power. This research and associated Decision Dominance Theory asserts that informational power is achieved through *controlling, exploiting, and enhancing information.*

Informational power achieves information advantage which secures decision dominance. Operations in the information environment set conditions for the physical environment. Informational power combined with physical power creates military power.

Recommendation 2: The US military requires organizational, leadership, and cultural change to achieve informational power and decision dominance. Information systems and intelligence architectures must be integrated across all echelons – tactical, operational, and strategic. Tactical mission planning and broader operational planning must shift to place information at the forefront of planning. Individuals and teams must understand the importance of operations in the information environment and the ways in which those operations shape the conditions in the physical environment. Formalized leader development and professional military education must emphasize the cognitive shift away from the traditional understanding of conflict as physical power and incorporate informational power and activities into planning, orders, and execution. Greater emphasis should be placed on understanding how to use and trust information, how to manipulate and process it into intelligence, and how it can be used to achieve decision dominance. Finally, digital literacy should be a requirement in future training.

Recommendation 3: JADO requires the ability to assess measures of performance and measures of effectiveness in the information environment. An effective assessment process must be developed to understand and measure the impact of operations in the information environment. This should be examined in more detail as it will build trust and provide a better understanding of how information warfare and information-related activities can generate military power and operational success.

Recommendation 4: Future command and control processes should enable the integration of planning and execution of operations in the information environment. A JADO military power plan should be developed to coordinate and direct strategy across all-domains and to execute operations in the information environment. This process should be integrated, not separated, from the physical and kinetic planning as information and information-related

activities shape and set conditions for the physical operating environment. A centralized planning process for operations in the information environment and operations in the physical environment is required to effectively integrate capabilities and effects.

Conclusion

Inter-state competition, coupled with the decline in traditional armed conflict, necessitates a shift in military thinking, organization, and operational approach. JADO requires a fundamental transference in thinking about combat operations. In modern warfare, combat operations require a deliberately crafted approach that combines informational and physical power. Operations in the information environment generate, apply, and alter information to change perceptions, attitudes, and decision-making of the adversary. The combination of these outcomes changes the course of events in the physical environment. Operations in the information environment can corrupt, slow, and paralyze an adversary's decision-making cycle. This paper asserts that deliberate action taken to target the enemy's cognitive and information filters will impede the adversary's decision-making process and deprive him of the ability to make informed decisions about effectively employing combat power. Achieving decision dominance requires pinpointed action in the information environment to set conditions for successful physical and all-domain operations.

Decision Dominance is achieved through informational power. Informational Power, attained through the combination of *controlling information, exploiting information, and enhancing information*, allows for the persistent, flexible, and adaptable application of information warfare capabilities in the information environment. These outcomes target the cognitive processes, information systems, and intelligence architecture of the adversary. By manipulating, controlling, or altering the adversary's decision-making system, one can deprive him of the capability to make decisions in his best interest. Removing the sanctuary of time and reducing or complicating the adversary's options reduces overall military capability.

This paper articulates that in order for the US military to prevail in competition and future conflict, it is imperative that the Joint Force understand how its adversaries operate in the information environment, and that the Joint Force must further develop its own operations in the information environment. Russia's information warfare strategy and its use of Reflexive Control demonstrate the vulnerability of operations in the information environment. Through active measures, Russia continuously strives to propagate discontent, cause confusion, and manipulate information to its own benefit. Russia controls and influences populations, legalizes its actions, creates ambiguity regarding its true intentions, and sets conditions to achieve its objectives with minimal physical power or confrontation using the information environment.

The implications of these findings necessitate a careful evaluation of how the Joint Force thinks and conducts operations. Coordinated and detailed planning must take place in the information environment. The Joint Force should put a greater emphasis on planning and coordinating operations to *control, exploit and enhance information* to achieve the information advantage and secure decision dominance. Operations in the information environment set conditions for the physical environment. Informational power combined with physical power creates military power.

The US military's understanding of the information environment and how the adversary attempts to exploit it is required to safeguard US interests and execute military operations. The information environment spans across all-domains: air, space, cyber, land, and maritime. US military strategy and planning must integrate processes in the information environment into a coordinated military power plan that can be executed across the competition continuum. Doing so will reduce the adversary's ability to persistently control, manipulate, and manage inputs in the information environment and throughout the gray zone of conflict. Achieving decision dominance will reduce the adversary's ability to act in the information space, while providing the US with opportunities to gain accurate information, operate with less interference, make informed decisions, and influence outcomes to its benefit. Future JADO concept development must put

information and information warfare capabilities at the forefront of planning. *The successful application of joint all-domain operations requires informational power -- the ability to control, exploit, and enhance information – and gaining and maintaining decision dominance to outwit and control the enemy's decision-making.*

Bibliography

Ajir, Media, and Bethany Vailliant. "Russian Information Warfare: Implications for Deterrence Theory". *Strategic Studies Quarterly* Fall 2018, no. 12. 3 (Fall 2018): 70–89.

Blank, Stephen, and Richard Weitz. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*. Carlisle, PA: Strategic Studies Institute, 2010.

Bonnell, Victoria E., and George W. Breslauer. *Russa in the New Century: Stability or Disorder?* Boulder, CO: Westview Press, 2001.

Brantly, Aaron F., Nerea M. Cal, and Devlin P. Winkelstein. "Defending the Borderland: Ukraine Military Experiences with IO, Cyber and EW." Army Cyber Institute at West Point, 2017. Assessed 10 November 2020. https://cyberdefensereview.army.mil/Portals/6/Documents/UA%20Report%20Final%20AB.pdf

Buraway, Michael. "The Extended Case Method." *Sociological Theory* 16, no. 1 (1998): 4–33.

Charmaz, Kathy. *Constructing Grounded Theory*. 2nd Edition. Lost Angeles: SAGE Publications Ltd, 2014.

Cimbala, Stephen, and Peter Jacob Rainow. *Russian and Post Modern Deterrence: Military Power and Its Challenges for Security*. Dulles, Virginia: Potomac Books, Inc, 2007.

Cohen, Ariel, and Robert E. Hamilton. "The Russian Military and the Georgia War: Lessons and Implications." US Army War College, 2011. Accessed 13 September 2020. www.jstor.com/stable/resrep11808 JSTOR.

Connell, Mary Ellen, and Ryan Evans. "Russia's 'Ambiguous Warfare' and Implications for the US Marine Corps." CNA Analysis and Solutions, May 2015. Assessed on 10 November 2020. https://www.cna.org/cna_files/pdf/dop-2015-u-010447-final.pdf

Cronkhite, Amanda, Wenshuo Zhang, and Leslie Caughell. "#FakeNews in #NatSec: Handling Misinformation." *US Army War College Quarterly Parameters* 50, no. 1 (Spring 2020): 5–22.

Deibler, Jeremiah. "Winning Wars of Cognition: Posturing the Air Force for the Tactical Information Fight." Accessed 13 September 2020. https://othjournal.com/2020/02/10/winning-wars-of-cognition-posturing-the-air-force-for-the-tactical-information-fight/.

De Spiegeleire, Stephan, Iuliia Solodovnik, and Nicholas Farnham. "Conflict and Cooperation." The Hague Centre for Strategic Studies, 2017. Accessed 20 July 2020. http://www.jstor.com/stable/resrep12572.

Deputy Commandant, Combat Development and Integration, and Deputy Commandant for Information. *Definitions of Information Related Terms*. Washington, DC: US Marine Corps, September 2020.

Dilworth, John. "The Reflexive Theory of Perception." *Behavior and Philosophy* 33 (2005): 17–40.

Fogarty, Stephen G., and Bryan Sparling. "Enabling the Army in an Era of Information Warfare." *The Cyber Defense Review* 5, no. 2 (Summer 2020): 17–28.

Gerasimov, Valery. "The Value of Science in Prediction." *Military-Industrial Kurier* (February 27, 2013).

Gleick, James. *The Information: A History, A Theory, A Flood*. NY: Vintage Books, 2011.

Harris, Shane, Ellen Nakashima, and Josh Dawsey. "Russia Is Trying to 'denigrate' Biden While China Prefers 'Unpredictable' Trump Not Be Reelected, Senior U.S. Intelligence Official Says." *The Washington Post*. NJ, August 7, 2020. Accessed 7 August 2020. https://www.washingtonpost.com/national-security/seeing-trump-as-unpredictable-china-would-prefer-he-not-win-reelection-intelligence-official-says/2020/08/07/98e1ad8c-d8e0-11ea-aff6-220dd3a14741_story.html.

Haugh, Timothy D., Nicholas Hall, and Eugene Fan. "16th Air Force and Convergence for Information Warfare." *Cyber Defense Review*, no. Summer 2020 (July 27, 2020): 29–43.

Headquarters US Air Force. "C2 of Operations in the Information Environment (OIE) Working Group." Washington, DC, HAF A3, May 1, 2020.

ISPI. "Means, goals and consequences of the pro-Kremlin disinformation campaign." Text. *ISPI*. Last modified January 19, 2017. Accessed 2 September 2020. https://www.ispionline.it/it/pubblicazione/means-goals-and-consequences-pro-kremlin-disinformation-campaign-16216.

Jerit, Jennifer, Jason Barabas, and Toby Bolsen. "Citizens, Knowledge and the Information Environment." *American Journal of Political Science* 50, no. No. 2 (April 2006): 266–282.

Jegelevicius, Linas. "In Lithuania, Russia's War for Influence Is Waged with Cable TV and Basketball." EuroNews, October 13, 2020. Accessed13 December 2020. https://www.euronews.com/2020/10/13/in-lithuania-russia-s-war-for-influence-is-waged-with-cable-tv-and-basketball.

Kasapoglu, Can. "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control." *National Defense College* 121, no. November 2015.

Kelly, Mark. *Strategic Multilayer Assessment (SMA) on Command and Control of Operations in the Information Environment*. Washington, DC: HAF A3, 2020.

King. "Reflexive Control and Disinformation in Putin's Wars." Graduate Theses & Dissertations, University of Colorado, 2018. Accessed 27 August 2020. https://scholar.colorado.edu/gsll_gradetds/27.

Kleckova, Adela. "Russia Targeting the Czech Republic over Statue Calls for International Reaction." The German Marshall Fund of the United States, May 2020. Assessed 1 December 2020. https://www.gmfus.org/sites/default/files/Russia%20Targeting%20the%20Czech%20Republic%20over%20Statue%20Calls%20for%20International%20Reaction.pdf.

Kliman, Daniel, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche. "Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations." Center for New American Security, May 2020. Accessed 4 October 2020. https://www.cnas.org/publications/reports/dangerous-synergies.

Krogerus, Mikael, and Roman Tschappeler. *50 Models for Strategic Thinking*. 2nd Edition. New York: W.W. Norton & Company, 2018.

McCauley, Kevin N. *Russian Influence Campaigns Against the West: From the Cold War to Putin.* SC: CreateSpace Independent Publishing Platform, 2016.

McFate, Sean. *The New Rules of War: Victory in the Age of Durable Disorder*. NY: Harper Collins Publishers, 2019.

Mulgund, Sandeep S., and Mark D. Kelly. *Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment*. Washington, DC: HAF A3, September 2020.

Pacepa, Ion Mihai, and Ronald J. Rychlak. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. Washington, DC: WND Books, 2013.

Paul, Christopher. "Understanding and Pursuing Information Advantage." *The Cyber Defense Review* 5, no. 2 (Summer 2020): 109–124.

Scott, William G., and Terence R. Mitchell. *Organization Theory: A Structural and Behaviorall Analysis*. 3rd Edition. Homewood, IL: Richard D. Irwin, Inc, 1976.

Shultz, Richard H., and Roy Godson. *Dezinformatsia: Active Measures in Soviet Strategy*. NY: Pergamon Press, 1984.

Stein, George J. "Information Warfare." *Airpower Journal*, no. IX (Spring 1995): 31–39.

Strategic Multilayer Assessment. "Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper." Washington Institute, May 2019. Accessed 31 July 2020. https://www.washingtoninstitute.org/uploads/Documents/opeds/Borshchevskaya20190503-SMA.pdf.

Snegovaya, Maria. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare." *Institute for the Study of War*, no. 1 (2015): 28.

Sybera, Albin. "Truth Missing in Action in Czech Information Wars." Balkan Insight. Sarajevo, September 19, 2019. Accessed 11 December 2020. https://balkaninsight.com/2019/09/09/truth-missing-in-action-in-czech-information-wars/.

Thomas, Timothy L. *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness*. Fort Leavenworth, KS: Foreign Military Studies Office, 2011.

———. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies*, no. 17 (2004): 237–256.

US Air Force. "Air Force Future Operating Concept: A View of the Air Force in 2035." Washington, DC: US Department of the Air Force, 2015. Accessed 17 July 2020. https://www.af.mil/Portals/1/images/airpower/AFFOC.pdf.

US Army Training and Doctrine Command (TRADOC). TRADOC Pamphlet 525-3-1, *The US Army in Multi-Domain Operations 2028*. Fort Eutis, VA: TRADOC, 2018. Accessed 28 July 2020. https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

US Army Cyber Center of Excellence. *Information Advantage: Expanded White Paper (Pre-Decisional).* Fort Gordon, GA: US Army Cyber Center of Excellence, 2020.

US Department of Defense. Joint Staff. Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*. Washington, DC: Government Publishing Office, 2017.

———. Joint Staff. *Joint Concept for Operating in the Information Environment (JCOIE).* Washington, DC: Government Publishing Office, 2018.

———. Joint Staff. J*oint Doctrine Note 1-19: Competition Continuum.* Washington, DC: Government Publishing Office, 2019.

———. Joint Staff. Joint Publication 2-0, *Joint Intelligence*. Washington, DC: Government Publishing Office, 2013.

———. Joint Staff. Joint Publication 3-0, *Joint Operations.* Washington, DC: Government Publishing Office, 2017.

———. Joint Staff. Joint Publication 3-13, *Information Operations*. Washington, DC: Government Publishing Office, 2014.

———. *Summary of the 2018 National Defense Strategy.* Washington, DC: Government Publishing Office, 2018.

US Department of the Air Force. Doctrine Annex. *Annex 3-1 Department of the Air Force Role in Joint All-Domain Operations (JADO)*. Maxwell AFB: Curtis E. LeMay Center for Doctrine Development and Education, 2020. Accessed 7 September 2020. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-1/Annex-3-1-DAF-Role-in-JADO.pdf.

Wardle, Claire, and Hossein Derakhshan. *INFORMATION DISORDER : Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe Report DGI, 2017. Accessed 31 July 2020. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

Widnall, Sheila E. "The State of the Air Force." *Airpower Journal*, no. IX (Spring 1995): 4–14.

Widnall, Sheila E., and Ronald R. Fogleman. *Cornerstones of Information Warfare.* Washington, DC: Department of the Air Force, April 1997.

Williams, Bruce A., and Michael X. Delli Carpini. *After Broadcast News: Media Regimes, Democracy, and the New Information Environment*. NY: Cambridge University Press, 2011.

Woody, Christopher. "Baltic States Think Russia Is Laying the Groundwork for Looking 'Kinetic Operations.'" *Business Insider*, April 3, 2017. Assessed 24 September 2020. https://www.businessinsider.com/russia-propaganda-in-lithuania-attack-on-the-baltics-2017-4.

Appendix

Table 1. Ground Theory Coding: - Open, Focused and Axial Coding

Open Coding: The following data represents the finding from Open Coding. Created by author.

Item: Media	**Item: Reflexive Control**	**Item: Gray Zone**	**Item: Astroturfing**
Source: Anderson, Jerit, Harris, Wardle. Ajir, Schultz	Source: Phillips, Kasapoglu, Thomas, King, McCauley	Source: Gerasimov, Connell	Source: Kliman, Wardle
Item: Audience	**Item: Cyber**	**Item: Inter-state competition**	**Item: Coercion**
Source: Jerit, Wardle	Source: Diebler, Ajir, King, McCauley	Source: NDS, 16 AF, MDO	Source: Kliman
Item: Information Battle / Conflict	**Item: Freedom of Movement**	**Item: Gerasimov Doctrine**	**Item: Information Operations**
Source: Thomas, Connell	Source: Krause, Kasapoglu	Source: Gerasimov, Cimbala, Connell, 16 AF	Source: Anderson, Cimbala, Wardle, Ajir, King, Connell, McCauley, Widnall, Mulgund
Item: 6th Generation (new generation)	**Item: Speed**	**Item: IRA**	**Item: Shape Perceptions**
Source: Gerasimov, Ajir, King, McCauley	Source: Gerasimov, Krause, Kasapoglu, Schultz	Source: Kliman, Phillips, 16 AF	Source: Kliman, Diebler, Krause, Thomas, McCauley
Item: Conventional	**Item: Information Pollution**	**Item: Information Tech**	**Item: Flooding**
Source: King	Source: Wardle	Source: Thomas, King, McCauley	Source: Kliman, Wardle
Item: Weaponize Information	**Item: Whole of Government**	**Item: Information Psychology**	**Item: Disinformation**
Source: Diebler, Wardle, Ajir, Thomas, King	Source: Phillips, Diebler, Kasapoglu, Ajir, Pacepa, 16 AF	Source: Ajir, Thomas, King, Connell, McCauley	Source: Kliman, Harris, Kasapoglu, Wardle, Ajir, Thomas, Pacepa, King, McCauley, Schultz
Item: Information Warfare	**Item: Degrade and Sow Discontent**	**Item: Cognitive Filter**	**Item: Exploit Divisions**
Source: Kliman, Diebler, King, 16 AF, McCauley, Widnall	Source: Kliman, Ajir, Connell, 16 AF	Source: Phillips, Diebler, Ajir, Thomas	Source: Kliman, King
Item: Target Decision Making	**Item: No Boundaries**	**Item: Information Disorder**	**Item: Legalism**
Source: Diebler, Krause, Kasapoglu, Ajir, Thomas, McCauley, Schultz	Source: Kliman, 16 AF, McCauley	Source: Wardle	Source: Hague, Harris, Kasapoglu, Connell

LEGEND – Decision Dominance Coding

Whole of Government	Information Warfare	Reflexive Control Theory	Tools (RCMethods)	Information Conflict	Information Firepower

Item: Constant Competition	**Item: Deconstruct**	**Item: False Messages**	**Item: Alter adversary's behavior**
Source: Krause, Mulgund	Source: Kliman	Source: Wardle, Ajir, King, Schultz	Source: JCOIE
Item: Divide Population and Audiences / Weaken Authority	**Item: Mask intentions**	**Item: Lobbyist**	**Item: Info is key terrain**
Source:	Source: Kasapoglu, King	Source: Ajir	Source: JCOIE
Item: No distinction b/w Peace and War	**Item: Create fog / friction**	**Item: NGOs**	**Item: Understand how the adversary assigns meaning**
Source: Gerasimov, Kliman, Ajir, Connell, McCauley	Source: Diebler, Krause, Kasapoglu	Source: Ajir, Thomas, Pacepa, Schultz	Source: JCOIE, Krause
Item: SOF Contractors	**Item: Alter analytical results**	**Item: Information Power**	**Item: What is the adversary's worldview?**
Source: Kasapoglu, Connell	Source: Kasapoglu	Source: JCOIE, Diebler	Source: JCOIE, Anderson
Item: A2Ad	**Item: Deep Penetration**	**Item: Protect observations**	**Item: Convergence**
Source: Kasapoglu	Source: Kasapoglu, Connell	Source: JCOIE, Paul	Source: 16 AF, MDO
Item: Model reasoning of the target	**Item: Target mind and systems**	**Item: MX / Change observations**	**Item: Conflict under the threshold of armed conflict**
Source: Thomas, 16 AF	Source: Ajir, Thomas	Source: JCOIE	Source: MDO, 16 AF, Ajir, Connell, 16 AF
Item: Control decisions of the enemy	**Item: Understand the OE**	**Item: Acquire, PED, Employ Data**	**Item: Global**
Source: Phillips, Diebler, Kasapoglu, Thomas, McCauley	Source: Krause, Thomas, JCOIE, McCauley	Source: JCOIE	Source: 16 AF, McCauley
Item: Get into intel apparatus	**Item: Damage info processors, systems and resources**	**Item: Increase combat power**	**Item: Flexibility**
Source: Kasapoglu	Source: Diebler, Ajir, Thomas, King, Widnall	Source: JCOIE	Source: 16 AF, Schultz

LEGEND – Decision Dominance Coding

Whole of Government	Information Warfare	Reflexive Control Theory	Tools (RCMethods)	Information Conflict	Information Firepower

Item: Persistent (Continuous)	**Item: Alter Algorithm**	**Item: Info as a joint function**	**Item: LR weapons (no contact, precision)**
Source: Thomas, King, 16 AF, McCauley	Source: Thomas, King, Schultz	Source: JP 3-0; JCOIE, Paul, Marine (Doc)	Source: Gerasimov, King
Item: Outcomes	**Item: Alter time**	**Item: Active Measures**	**Item: reduce time, space and info gaps**
Source: 16 AF	Source: Thomas	Source: Anderson, Wardle, McCauley, Ajir, McCauley	Source: Gerasimov
Item: Increase IO	**Item: Manipulate message and target**	**Item: Propaganda**	**Item: simultaneous action**
Source: Thomas, 16 AF	Source: Krause, Kasapoglu, Ajir, King, JCOIE	Source: Anderson, Wardle, Ajir, McCauley, Schultz	Source: Gerasimov
Item: War of Cognition	**Item: EBO**	**Item: Legitimize Power**	**Item: War not declared**
Source: Phillips, Deibler, CSAF	Source: Krause	Source: Anderson, Kliman	Source: Gerasimov, Phillips
Item: Environment = IE + OE	**Item: Prevent sensor from seeing**	**Item: Info is part of foreign policy**	**Item: find the enemy vulnerability**
Source: Diebler, Thomas	Source: Diebler, Paul	Source: Anderson, Ajir	Source: Gerasimov, Connell
Item: Great Power Competition (RUS + CHN)	**Item: promote mistaken conclusion**	**Item: LR Strike**	**Item: military action as last resort**
Source: SMA white paper	Source: Diebler, Paul	Source: King	Source: Gerasimov, Phillips, Diebler, King, Connell
Item: Combined Fires	**Item: Corrupt / slow OODA loop**	**Item: reduce enemy fighting potential**	**Item: New Warfare & Asymmetric Advances**
Source: Diebler, Thomas	Source: Krause, Paul	Source: Gerasimov	Source: Gerasimov, Phillips, Krause, Ajir, McCauley, McCauley
Item: FDO/FRO	**Item: destroy or discredit source credibility (make your own source credible)**	**Item: unified information space**	**Item: IW Operations**
Source: Thomas	Source: Wardle, Paul, Ajir, Thomas, King, Schultz	Source: Gerasimov, McCauley	Source: Gautheier, Thomas

LEGEND – Decision Dominance Coding

Whole of Government	Information Warfare	Reflexive Control Theory	Tools (RCMethods)	Information Conflict	Information Firepower

Item: IW C2	**Item: harass and confuse**	**Item: Hybrid warfare**	**Item: Sixth Domain (Cognitive / human)**
Source: Gautheier, Thomas, Connell	Source: Gautheier, Thomas	Source: Kasapoglu, King, Connell, Schultz	Source: Ajir
Item: IW Technology	**Item: Disrupt DM**	**Item: Full spectrum**	**Item: Kernel of Truth**
Source: Gautheier, Thomas	Source: Gautheier, Krause, Thomas, McCauley	Source: Kasapoglu	Source: Pacepa
Item: Asymmetric	**Item: Types of Knowledge - General, Domain, Surveillance**	**Item: Permanent Readiness**	**Item: Time, platform, location, duration**
Source: Gautheier, Ajir, King, McCauley	Source: Jerit	Source: Kasapoglu	Source: JCOIE
Item: Information Deterrence	**Item: Make choices based on values and beliefs and motives**	**Item: Subversion**	**Items: Shared context**
Source: Gautheier	Source: Jerit, Phillips, Krause, Wardle	Source: Kasapoglu, King, Connell, McCauley	Source: JCOIE
Item: Information weapons (COTS)	**Item: Information is firepower**	**Item: Manipulate sensory awareness**	**Item: understand relevant actors**
Source: Gautheier, Thomas	Source: Kliman, Diebler, Wardle, Thomas	Source: Kasapoglu	Source: JCOIE
Item: attack enemy C2	**Item: Trolls and Bots**	**Item: Sow mistrust and confusion**	**Item: understand change**
Source: Gautheier	Source: Kliman, Wardle, Ajir, 16 AF	Source: Wardle	Source: JCOIE
Item: destroy eyes and ears	**Item: Amplify the narrative**	**Item: avoid exposing friendly plan**	**Item: Information Environment**
Source: Gautheier, Diebler, Paul	Source: Kliman, Wardle, King	Source: Paul	Source: JCOIE
Item: Deception and concealment	**Item: Denial of open military force**	**Item: Influence**	**Item: Image Recognition**
Source: Gautheier, Ajir, Thomas, Connell, McCauley	Source: Kasapoglu	Source: Kasapoglu, Ajir, Thomas, King, McCauley	Source: Schultz, Thomas

LEGEND – Decision Dominance Coding

Whole of Government	Information Warfare	Reflexive Control Theory	Tools (RCMethods)	Information Conflict	Information Firepower

Item: information technology to increase speed and transmission	**Item: Counterinformation**	**Item: Operations, Activities and Investments (OAI)**	**Item: Campaign Activities - Assure, Deter, Induce, Compel**
Source: Widnall	Source: Widnall	Source, Mulgund	Source: Mulgund
Item: Information as decisive	**Item: Paralyze the enemy's ability to C2**	**Item: Attack and defend information**	**Item: Information uses - inform, influence, attack and exploit**
Source: Widnall	Source: Widnall	Source: Widnall	Source: Mulgund
Item: Information = observed phenomenon + process (context)	**Item: Info as a target**	**Item: Exploit Information**	**Item: Informational Power**
Source: Widnall	Source: Widnall	Source: Widnall	Source: JCOIE, Mulgund
Item: Direct & Indirect IW	**Item: Physical Power**	**Item: Info Attack (C2 Attack) to perserve resources**	**Item: Campaign Design**
Source: Widnall	Source: Mulgund	Source: Widnall	Source: Mulgund
Item: IW Objectives - Control, Exploit, Enhance			
Source: Widnall			

LEGEND – Decision Dominance Coding

Whole of Government	Information Warfare	Reflexive Control Theory	Tools (RCMethods)	Information Conflict	Information Firepower

Focused and Axial Coding: The following data a represents the finds from the focused and axial coding. Created by author.

Focused	Axial (Who, What, Where, When, Why)		
	Conditions: situation or circumstance that form the structure of phenomena (Why? Where? How come? When?)	Actions / Interactions: participants routine or strategic responses to issues, events or problems (By Whom? How questions?)	Consequences: outcomes of actions/interactions (What happens as a result?)
Whole of Government (WoG)	1 - Gray Zone 2 - Global 3- Inter-state competition 4 - Continuous 5 - Legalism (Masked Intentions) 6 - Info is part of foreign policy	1 - Legitimize Power 2 - Deny forcible action 3 - Legalization of action 4 - Deliberate, planned and calculated action to minimize escalation to armed conflict	1 - MX operations under the threshold of armed conflict 2 - Environment = IE + OE 3- No distinction between peace and war 4 - Shift worldview
Information Warfare (IW)	1 - Outcomes Focused 2 - Information as a Joint Function 3 - Require integrated kinetic and non-kinetic effects 4 - Elements of IW 5 - Understanding of general, domain and surveillance knowledge (OE)	1 - US military, RUS 2 - How can information be used as a the new "firepower?" 3 - How can the US target the adversary's behavior? 4 - How do we understand relevant actor? 5 - How do we understand change? 6 - How do we control and exploit information to enhance military operations? (Campaign Design)	1 - Shared context 2 - Integrated EW, IO, ISR, Cyber Operations 3 - Reduced Time, Space, and Info Gaps 4 - Integrated tech spt and C2 for integrated IW outcomes 5 - Focused targeting directed at adversary's values, beliefs, and motives
Reflexive Control Theory (RCT)	1 - Desire to control the narrative 2 - Desire to influence population 3 - Desire to shape perceptions, attitudes and decision of a decision makers	1 - Acquire, PED and employ data against the adversary 2 - Conduct deception (disinformation, misinformation, malinformation) to manipulate target ("Kernel of Truth") 3 - Identify, deconstruct, and target the adversary's cognitive filter 4 - Focused efforts on information technology (systems) and information psychology (minds) of the adversary 5 - How does the adversary assign meaning? 6 - What is the adversary's worldview? 7 - How do you manipulate the adversary's sensory awareness?	1 - Disrupted decision makers processes (OODA loop) 2 - Exploited divisions and fissures withing target audience 3 - Modeled reasoning of the target 4 - Altered perceptions and actions, mistaken conclusions 5 - Information is a "weapon"

LEGEND – Decision Dominance Coding

Whole of Government	Information Warfare	Reflexive Control Theory	Tools (RCMethods)	Information Conflict	Information Firepower

Tools (T) (RC Methods)	1 - Desire to control and influence the population or decision maker (designated audience) 2 - Provide negative or positive interactions on a global scale 3 - Desire to understand the IE and OE 4 - Target the adversary's vulnerability	1 - Cyber actions 2 - Media Influence 3 - Flooding / Info Pollution 4 - Disinformation (False Messages) 5 - Astroturfing 6 - IRA, Trolls, and Bots (amplification) 7 - Use of lobbyists and NGOs 8 - Destroy / discredit source 9 - Active Measures 10 - Propaganda 11 - Deception and Concealment 12 - Harass, confuse, sow distrust within target audience 13 - OPSEC 14 - Image Recognition	1- Divide population (audience) 2 - Weaken Authority 3 - Mask Intentions 4 - Create Fog and Friction 5 - Deep Penetration 6 - Access to intel apparatus 7 - Alter analytical results 8 - Damage / disrupt info systems, processors, and resources 9 - Prevent sensor from "seeing" or "hearing"
Information Conflict (IC)	1 - Constant competition 2 - Global reach, flexibility and persistence 3 - Gray Zone	1 - Next Gen / Sixth Gen Warfare 2 - Development of LR, precision, standoff weapons 3 - Focus on information actions to null military weapons	1 - Weaponize Information 2 - All Domain Operations 3 - Hybrid operations 4 - Limited kinetic action (last resort) 5 - A2AD standoff
Info Firepower (IF)	1 - competition has given rise to fewer military conflicts 2 - information is used on a continuous basis to target populations, militaries and decision makers 3 - Well placed information can control and influence a target audience or decision maker 4 - Denying the adversary the ability to make smart and informed decision requires actions in the information environment	1 - allows actor to protect and MX observations 2 - OPSEC 3 - Simultaneous EW, ISR, IO and Cyber actions 4 - How do we control and exploit information to shape the physical environment and perserve resources / action?	1 - Preserves Freedom of Movement 2 - Preserves time and action (Information Power) 3 - Corrupts / degrades adversary's OODA Loop; impairs adversary's ability to C2 4 - Allows for increased speed 5 - Convergence (all-domain and simultaneous effects) to maximize combat power 6 - Alter adversaries behavior and decision algorithm 7 - Combined Fires / Unified Information Space 8 - Reduce adversary's fighting protentional 9 - Information is decisive

LEGEND – Decision Dominance Coding

Whole of Government | Information Warfare | Reflexive Control Theory | Tools (RCMethods) | Information Conflict | Information Firepower