# WEAPONIZED NARRATIVE:

# EXPLORING NEW VOCABULARY FOR THE COGNITIVE DOMAIN FIGHT

BY

CALVIN PETERSON, JR.

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2018

## APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

MELVIN R. KORSMO, PhD, Lt Col, USAF (Date)

JAMES D. KIRAS, PhD (Date)

# DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

## ABOUT THE AUTHOR

Maj Calvin E. Peterson Jr. received his commission in 2004 as a graduate of the U.S. Air Force Academy, Colorado. He has served in operational units filling key leadership positions to include Assistant Director of Operations, numerous Flight Commander positions, Chief of Mobility, Chief of Training, and project officer for multiple CENTCOM deployments. Maj Peterson is a senior pilot with over 1,400 flying hours contributing to contingency operations during NATO Icelandic Air Policing, NATO Baltic Air Policing, Operation NOBLE ENDEAVOR, and a CENTCOM Theater Security Package. He has flown as an instructor pilot in the F-22, 4 Ship Flight Lead in the F-15C, and as a T-38 Evaluator Pilot for ACC's first T-38 Adversary Program.

Prior to attending the School of Advanced Air and Space Studies, he was a student at the Army Command and General Staff College, Fort Leavenworth, KS. Major Peterson holds a Bachelor of Science degree in Management from the U.S. Air Force Academy, and a Master of Business Administration from Trident University International.

# ACKNOWLEDGMENTS

I would like to acknowledge several people whose support, patience, and encouragement were critical to this study. First, and most importantly, I want to express my sincere gratefulness to my wife and kids for their enduring love and uplifting spirit during days, nights and weekends spent researching and writing this paper. My wife read and edited each page and listened to me explain my muddled thoughts late at night. She never once complained during my lengthy absentminded times at home, and always greeted me with a smile, joy, and inspiration.

I want to thank Lt Col Melvin Korsmo, my thesis advisor, for his time and patience during many discussions spent funneling my thoughts to resemble an identifiable structure. His willingness to educate and provide insightful references was instrumental to my study and personal growth. I thank Dr. Kiras for his encouragement throughout the year, reviewing the draft and providing valuable feedback. I would also like to thank all my SAASS course instructors—Dr. Tucci, Dr. Hughes, Dr. Benson, Dr. Muller, Dr. Pfannenstiel, and Col Lowenthal—who all inspired portions of this study.

I also want to thank Jeffrey Kubiak, Professor and Senior Fellow at Arizona State University, for his excitement and encouragement for my project. He was the "belly button" to receive critical insights and feedback from the leaders and brain trust of Arizona State University's Weaponized Narrative Initiative.

# ABSTRACT

The US lacks a sufficient lexicon for fully comprehending cognitive threats as the character of warfare and conflict changes in the information age. The current lexicon of cognitive domain terms—propaganda, disinformation, information operations, MISO, PSYOP, military deception, and cognitive hacking—is insufficient for identifying and communicating intricate cognitive threats and for formulating an appropriate strategy in response to them.

This study explores the value of a newly proposed term—*Weaponized Narrative*—first coined by Braden Allenby in January 2017. The study modifies Allenby's original conception, contending that Weaponized Narrative is best understood as *the use of story-based communication to foment political and social schisms with the intent of subverting an adversaries' institutions, identities, and/or will*.

The objective of this project is primarily twofold: First, it aims to extract the distinct attributes of Weaponized Narrative. This aim is accomplished by comparing and contrasting the contextual definition provided above with other common terminology used to describe and understand the cognitive battlespace. Second, the project considers how these qualities explain recent Russian cognitive influence activities in the US. Two sets of cases are examined, including: 1) Russia's meddling in the US 2016 Presidential Election; and 2) Russia's manipulation of pre-existing socio-political divides, with examples found in cases like Black Lives Matter and Hearts of Texas versus the United Muslims of America.

The paper concludes with a discussion about how Weaponized Narrative presents a unique challenge to democracies that struggle to thwart foreign meddling while preserving democratic values of equality and liberty. Additionally, it proposes a revival of an appropriately-scoped entity that can actively lead, manage, and optimize the US information instrument of power.

# CONTENTS

Chapter Page

## Illustrations

Table Page

Figure Page

# Chapter 1

## Introduction

> *The target of all human conflict, the battleground of all conflict resolution, is the human mind… Conceptions of security or insecurity exist in the mind.*
>
> Richard Szafranski

> *America's competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information. They exploit marketing techniques to target individuals based upon their activities, interests, opinions, and values. They disseminate misinformation and propaganda. Risks to U.S. national security will grow as competitors integrate information derived from personal and commercial sources with intelligence collection and data analytic capabilities based on Artificial Intelligence (AI) and machine learning… U.S. efforts to counter the exploitation of information by rivals have been tepid and fragmented.*
>
> US National Security Strategy, Dec 2017

US information statecraft is failing to effectively recognize, communicate, and formulate strategies to counter cognitive threats. When scholars and practitioners describe the actions and events of recent Russian engagements in the US,[1] they commonly rely on highly abstract terms such as *information operation*, *propaganda*, and *disinformation*. Other descriptive terms, for example *themes* or *messages*, are more precise in that they detail a specific type of tool or action being used by a government. A few terms—such as *psychological operations* or *military deception*—carry an implied assumption of secrecy, meaning that only a countries' most elusive components of the

[1] Russian information operations in the US are ongoing and contentious. One recent example was *US military wives threatened by Russian hackers posing as ISIS* (an article published by Fifth Domain, May 8, 2018). A panel identified that the US is nowhere close to deterring Russian injection of disinformation in America (see John Grady's article, "Panel: U.S. Needs Non-Military Options to Handle 'Gray Zone' Warfare from Russia, China, Iran," *USNI News* (blog), May 15, 2018).

FBI, CIA, and military special operations can use them. Ultimately, none of these terms accurately capture the malignancy and severity of Russia's recent attacks in the cognitive domain.

Said differently, the current lexicon is insufficient to interpret and communicate cognitive domain threats in a succinct, clear, meaningful manner. A lexicon expansion is needed to effectively identify, communicate, and formulate strategies against cognitive domain threats such as Russian influence operations in the US. This bold claim necessitates defining several critical terms: First, the *cognitive domain*—also called the *cognitive realm*—is the mental action or process of acquiring knowledge and understanding through thought, experience, and the senses to generate perceptions, judgments, decision-making, and values. *Cognitive threats,* in turn, are unwanted influences in the cognitive domain that can alter behavior, decision-making, values, identity, and ultimately will.

A revised and expanded lexicon will address the US's cognitive capability gap, one evidenced by America's struggles to comprehend cognitive threats and craft strategies to protect the population from unwanted foreign informational influence. In an effort to articulate this gap and identify the threat, a Strategic Multi-Layer Assessment (SMA)[2] team conducted a yearlong study of Gray Zone[3] tactics used by adversaries around the world. The study produced a white paper entitled, *A Cognitive Capabilities Agenda: A Multi-Step Approach for Closing DoD's Cognitive Capability Gap*. The white paper claimed that "US mastery of physical domains has significantly outpaced proficiency in planning and operating effectively in the human cognitive domain…" and that its failure "to consider the cognitive, information space a core function of military

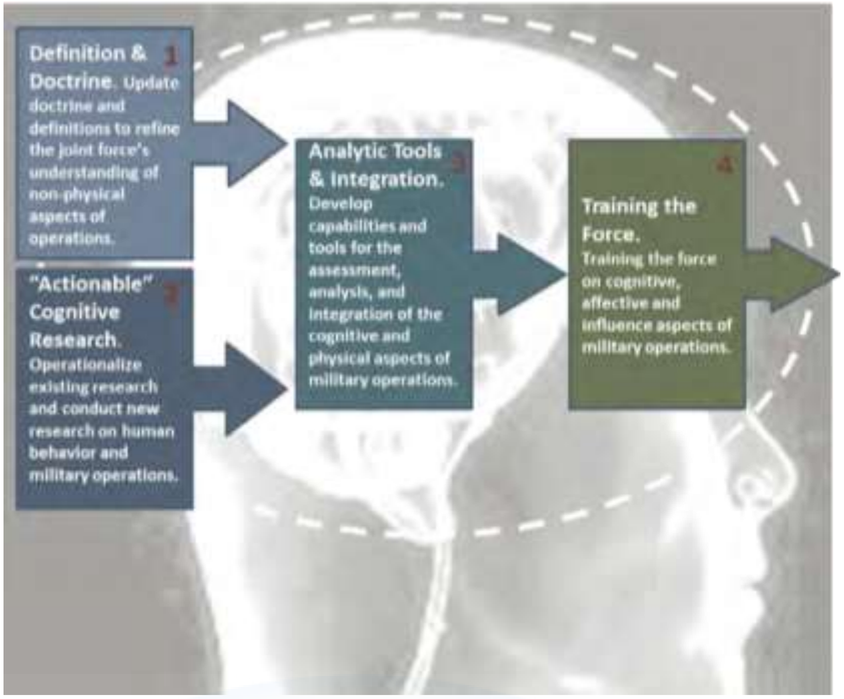
[2] The National Security Innovations (NSI) describes the US DoD SMA program as a "multidisciplinary, multi-agency portfolio of projects that studies and assesses challenging problems associated with planning and operations of DoD, military services, and government agencies. SMA is accepted and synchronized by Joint Staff/J-39 Directorate for Special Activities and Operations and executed by Assistant Secretary of Defense for Research & Engineering/Rapid Fielding Directorate/Rapid Reaction Technology Office." For further SMA details and description visit the NSI Inc website, http://nsiteam.com/sma-description/.

[3] For a description of Gray Zone see the Unconventional Warfare in the Gray Zone article published by National Defense University Press, January 1, 2016. The article characterizes Gray Zone as "intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."

operations, and not as a 'support activity' represents a significant vulnerability in US defense capabilities."[4]

The cognitive capability gap demonstrates the US failure to appreciate and understand the impact of cognitive operations as it relates to national security. An SMA team claimed there is "growing evidence that US adversaries have recognized the deficiency in US cognitive capabilities and have pursued ways to exploit it to their advantage via gray zone and other technologically-focused tactics." How can the US cognitive capability gap be closed or rectified? The SMA team provided a four-step set of recommendations for closing the gap: Step one: update definitions and doctrine; Step two: conduct actionable cognitive research; Step three: develop analytic tools and integration; Step four: train the force (see Figure 1).[5] This project primarily addresses the SMA's first recommended step, which advocates "the need to modernize traditional military definitions, doctrine, and understanding to acknowledge and include the overlooked human, cognitive domain."[6] The proposed new term, Weaponized Narrative, and the definition offered in this project—along with the application of that term and its definition to real-world examples—fulfills the first and most critical step in addressing America's lack of cognitive domain tools and responses.

[4] Allison Astorino-Courtois, ed. "A Cognitive Capabilities Agenda: A Multi-Step Approach for Closing DoD's Cognitive Capability Gap." Strategic Multi-Layer Assessment Office, October 2017.
[5] Allison Astorino-Courtois, ed. "A Cognitive Capabilities Agenda."
[6] Ibid.



1 Definition & Doctrine. Update doctrine and definitions to refine the joint force's understanding of non-physical aspects of operations.

2 "Actionable" Cognitive Research. Operationalize existing research and conduct new research on human behavior and military operations.

3 Analytic Tools & Integration. Develop capabilities and tools for the assessment, analysis, and integration of the cognitive and physical aspects of military operations.

4 Training the Force. Training the force on cognitive, affective and influence aspects of military operations.

**Figure 1: Closing the Cognitive Capability Gap**
Source: Allison Astorino-Courtois, ed. "A Cognitive Capabilities Agenda."

In January 2017, Braden Allenby, founding co-director of Arizona State University's Weaponized Narrative Initiative, proposed the term *Weaponized Narrative* as a modernized term for more accurately capturing actions and concepts occurring in the cognitive realm. Specifically, Weaponized Narrative helps with the lack of accurate terminology for distinguishing dangerous cognitive issues from non-events. Allenby's proposed definition is: *Weaponized Narrative is the use of story-based communication to foment political and social schisms with the intent of subverting an adversaries' institutions, identities, and/or will.*[7]

Weaponized Narrative is a strategy to gain a position of advantage in inter-state competition. The term "Weaponized Narrative" adds clarity and understanding to evasive threats in the changing character of war and conflict. The changing character concern is expressed by the US 2018 National Defense Strategy (NDS), which "acknowledges an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-

[7] This is a modified definition of the original proffered by Braden Allenby. See Chapter 2 for further explanation.

term, strategic competition between nations. These changes require a clear-eyed appraisal of the threats we face, acknowledgement of the changing character of warfare, and a transformation of how the Department conducts business."[8]

The term Weaponized Narrative provides a new perspective for identifying and communicating threats in inter-state long-term strategic competition. For example, the NDS presents an abstract claim that "China and Russia are now undermining the international order from within the system by exploiting its benefits while simultaneously undercutting its principles and 'rules of the road.'"[9] How is this occurring? That is, how are China and Russia exploiting benefits and undercutting principles? This new term provides a means by which to detect, identify, and respond to an adversary—thus filling a critical void.

Rapid technological advancements and the undeniable loss of the homeland as a sanctuary are additional concerns in the security environment expressed within the NDS.[10] Understanding the Weaponized Narrative term will show how advancing technologies are generating vulnerabilities in the cognitive domain. The NDS states, "America is a target, whether from terrorist seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion."[11] These targets, particularly information subversion, are precisely how revisionist powers will exploit ambiguity and blur the lines between civil and military defenses.[12] Weaponized Narrative is a way information subversion manifests in US homeland attacks.

Whether acknowledged or unacknowledged, cognitive capability gaps are a woven concern in the Department of Defense (DoD) objectives stated in the NDS.[13] In

[8] "Summary of the 2018 National Defense Strategy of The United States of America." Accessed February 1, 2018. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] There are 11 NDS Defense objectives. Cognitive capability gaps allow threats like Weaponized Narrative to challenge key NDS defense objectives, some of which include: Defending the homeland from attack; Deterring adversaries from aggression against our vital interests; Enabling U.S. interagency counterparts to advance U.S. influence and interests;

the publication Joint Concept for Human Aspects of Military Operations (JC-HAMO),[14] the recommendation to address cognitive capability gaps (see Figure 1) was mirrored by the SMA team's step one recommendation mentioned above. The JC-HAMO recommends to "inculcate an understanding and consideration of human aspects to enhance the design, planning, conduct, and assessment of military operations—and to achieve national policy objectives."[15] The Weaponized Narrative term is not the "silver bullet" answer to the concerns of the NDS, JC-HAMO, and SMA team, but it provides a way to clarify abstract thoughts and increase understanding of cognitive threats in inter-state competition.

The purpose of this paper is to explore the contextual meaning of Weaponized Narrative by addressing two critical questions: 1) What key qualities distinguish Weaponized Narrative? and 2) How do these qualities explain recent Russian cognitive influence activity in the US? The project's premise is that the term Weaponized Narrative is distinct from other pre-existing cognitive lexicon and partially fills the cognitive capability gap by bolstering communicative language to enhance comprehension of cognitive threats. The Weaponized Narrative term improves the ability to recognize, communicate, and formulate strategy in opposition to intricate cognitive threats as the character of warfare and conflict changes in the information age.

In support of these claims, the remainder of this paper is divided into six chapters. Chapter 2 defines Weaponized Narrative and provides layers of context that enrich comprehension of the newly proposed term. Chapter 2 suggests Weaponized Narrative is a strategy and discusses the expanding cognitive battleground generated by blind faith

Maintaining favorable regional balances of power in the Indo-Pacific, Europe, the Middle East, and the Western Hemisphere; Ensuring common domains remain open and free. For a complete list of defense objectives reference the "Summary of the 2018 National Defense Strategy."

[14] The purpose of JC-HAMO is to focus "the future Joint Force on a critical and enduring challenge in warfare—the need to understand relevant actors' motivations and the underpinnings of their will…the intent of JC- HAMO is to revise the manner in which the Joint Force thinks about and addresses human aspects, while strengthening the application of operational art. The JC-HAMO mindset and approach is critical to producing enduring strategic outcomes. All echelons of our force must have a foundational understanding of what drives human behavior. As each Military Service and a range of other stakeholders contributed to the evolution of this concept, the entire force must now play a role in its implementation." US Joint Chief of Staffs, "Joint Concept for Human Aspects of Military Operations," October 19, 2016.

[15] US Joint Chief of Staffs, "Joint Concept for Human Aspects of Military Operations." October 19, 2016.

many US citizens place in contemporary communication technologies. Chapter 3 juxtaposes Weaponized Narrative with other cognitive domain terms to establish similarities and differences in their qualities and characteristics. Chapters 4 and 5 provide evidence of Weaponized Narrative's existence by examining Russian meddling before, during, and after the 2016 US presidential election. Chapter 6 discusses the relevance of Weaponized Narrative in international relations. This chapter correlates Weaponized Narrative with state power, describes ambiguity in international law, and points out unique considerations for democracies attempting to wield or respond to it. Chapter 7 concludes the paper by emphasizing the important uses of the Weaponized Narrative term, followed by potential approaches to addressing the problems represented by the term.

# Chapter 2

## Defining and Contextualizing Weaponized Narrative

The purpose of this chapter is to define Weaponized Narrative and provide a contextual explanation of the term. To accomplish this task, the chapter is organized into four sections: The first section evaluates the commonly referenced definition of Weaponized Narrative as given by Braden Allenby. A modified and truncated version of Allenby's definition is then proposed. Section two briefly discusses the impact of narrative on societies and culture. The third section examines Weaponized Narrative as a strategy by using descriptions from Carl von Clausewitz's theory of war. Section four explains why human faith in algorithms and machine learning have expanded cognitive battleground and contributed to the rising relevance of Weaponized Narrative.

### Section 1: Definition of Weaponized Narrative

An advisable first step for understanding Weaponized Narrative is to parse the two terms and consider their individual lexical definitions. The Merriam-Webster Dictionary defines *weaponize* as adapting something "for use as a weapon of war,"[1] while *narrative* refers to a communicative, detailed, and often spoken account of connected events, or a story.[2] So then, at its simplest, Weaponized Narrative is a detailed story used as a weapon of war.

The combined term did not arise until January 2017, when Braden Allenby and Joel Garreau offered it in their article, "Weaponized Narrative Is The New Battlespace." In presenting this neologism, Allenby offered an initial definition, concluding in a white paper that Weaponized Narrative is "the use of disinformation, fake news, social media, and other information and communication technologies to create stories intended to subvert and undermine an adversary's institutions, identity, civilization and will by creating and exacerbating complexity, confusion, and political and social schisms."[3]

[1] "Weaponize | Definition of Weaponize by Merriam-Webster." Accessed October 6, 2017. https://www.merriam-webster.com/dictionary/weaponize.
[2] Ibid.
[3] Braden Allenby, "White Paper on Weaponized Narrative." June 2017. https://weaponizednarrative.asu.edu/publications/weaponized-narrative-white-paper-0. Allenby

Allenby's definition serviceably reaches beyond the initial definition above by denoting the importance of three structural components: namely *medium*, *method,* and *intent/objective*.

These three key components convert an otherwise nebulous concept into an understandable and executable strategy. Retired US Army Colonel and Professor at the Army War College, Art Lykke, crafted a strategy paradigm that assimilated a balance of ends, means, and ways to minimize risk[4] in the achievement of desired objectives.[5] The *intent* (ends) of Weaponized Narrative is achieved by the *method* (ways) based on the available *medium* (means). Each of these three key structural components of *medium, method,* and *intent/objective* is described briefly below, along with the limitations of Allenby's proposed definition.

*Medium* is the delivery platforms and products used to convey Weaponized Narratives. In other words, media are where someone would look for Weaponized Narratives. Media include the broad range of all forms of communication, including oral, written, and body language. Delivery platform examples include TV, radio, prints, music/songs, and the internet. Examples of products carried by these platforms are stories, truth, lies, facts, disinformation, themes, and messages. Concerning different delivery platforms and products on those platforms, Allenby's definition specifically refers to "disinformation, fake news, social media, and other information and

later articulated two important exclusions to his original definition. In the article entitled, *The Age of Weaponized Narrative,* Allenby stated, "First, commercial and nongeopolitical [sic] narratives are generally excluded, although of course the insights from such domains can be rapidly integrated into weaponized narratives. The second exclusion contains narratives intended for internal audiences, either to consolidate or maintain power. The Nazi Germany and Soviet examples of the Big Lie, or modern examples such as the narratives of Mother Russia and religious orthodoxy supporting Russian president Vladimir Putin's regime, are thus excluded." These exclusions reserve Weaponized Narrative as a tool for affecting external rather than domestic or commercial audiences.

[4] *Risk* is the fourth element of Lykke's strategy paradigm and it is also an element of Weaponized Narrative. If ends, ways, and means were a three-legged stool, any angular offset of the stool seat generated from uneven legs would represent the risk involved in the paradigm. Angular offset of the stool seat, or risk, should be minimized while recognizing that there will always be some risk to strategy. Weaponized Narrative is not impervious to risk; an imbalanced application can result in blowback for the user or the strengthening of an adversary, which is the exact opposite of the desired effects. Some stories or narratives are simply unpredictable because human emotion and reasoning can produce unexpected perceptions and misperceptions.

[5] H. Richard Yarger, "Towards A Theory of Strategy:" Accessed April 15, 2018. http://www.au.af.mil/au/awc/awcgate/army-usawc/stratpap.htm.

communication technologies."[6] Naming specific elements helps in identifying and applying the definition. Such terms, however, should reside in description rather than in definition for two reasons: 1) Listing some platforms and products, while excluding others calls into question why such decisions were made; and 2) This anchors the definition with contemporary terms. The staggering, rapid pace of development in information and communication technologies will likely lead to significant shifts in which platforms and products are leveraged in the future.

The *methods* of Weaponized Narrative describe "how" to achieve the intent/objective, and equate to the *ways* in Lykke's ends-ways-means-risk paradigm of strategy. Defined by Allenby, methods are creating or exacerbating stories, complexity, confusion, and schisms. These methods provide observable and measurable areas to evaluate effectiveness. Allenby's definition, unfortunately, splits the method (italicized here for emphasis) into two sections, arguing that Weaponized Narrative is used "*to create stories* intended to subvert and undermine an adversary's institutions, identity, civilization and will *by creating and exacerbating* complexity, confusion, and political and social schisms." This split of the applied methods induces unnecessary confusion into the definition. Selecting media and the amalgamation of truth, facts, lies, and deceit to foment schisms depend on the user's objectives.

The *intent* of Weaponized Narrative is to subvert and undermine an adversary's institutions, groups, identities, cultures, and/or will. An actor's intent could be the desire to increase its power or prestige by subverting an adversary, or simply subvert an adversary without concern for its power or prestige. Objectives can range from the minor weakening of an adversary to the full destruction of an adversary or its associated allies. Explaining why an actor would use Weaponized Narrative is only limited by human emotion and reasoning.

Perception and misperception are at the core of assessing intent. Cognitive dissonance is a significant reason why determining the intent in Weaponized Narrative can be difficult. The argument in the theory of cognitive dissonance is "that people seek to justify their own behavior-to reassure themselves that they have made the best possible use of all the information they had or should have had, to believe that they have not used

[6] Braden Allenby, "White Paper on Weaponized Narrative."

their resources foolishly, to see that their actions are commendable and consistent."[7] The stories in Weaponized Narrative can piggyback on very truthful opinions and viewpoints, some of which can be part of existing narratives created or supported by leaders. Cognitive dissonance would explain why a hijacked narrative would not be assessed as a contributor to schisms if attributed to an adversary intending to subvert institutions, identity, and/or will.

The challenge of assessing intent is also a strength Weaponized Narrative brings to the cognitive domain. Weaponized Narrative adds another category of intent. Most cognitive domain terms revolve around the intent to change behavior or decision-making for the benefit of the user. The intent of Weaponized Narrative adds potency—to subvert, undermine, degrade, or destroy—and using the term would force further analysis and questions about the objectives and motives of adversaries. For this reason, Weaponized Narrative can aid in reducing cognitive dissonance by allowing avenues of inquiry that break collective trains of thought, play devil's advocate, and avoid the trap of believing that adversaries see their actions as the opposition would see them.

Based on the challenges noted above I propose a condensed, simplified, and reorganized version of Allenby's definition for use throughout the remainder of this paper: ***Weaponized Narrative is the use of story-based communication to foment political and social schisms with the intent of subverting an adversaries' institutions, identities, and/or will***. The inclusion of Weaponized Narrative in the repertoire of cognitive lexicon adds a new perceptive tool to analyze cognitive attacks through a systematic approach of medium, method, and intent.

### The Overuse of the term 'Weaponized'

If "weaponized" is persistently and unthoughtfully adjoined with a host of other terms, its effectiveness as a modifier becomes diluted as people become desensitized to the term. Instead, this clarifying term ought to spark critical thinking about the grave repercussions of using weapons in competition, conflict, or war. In the article, "If Everything Can Be 'Weaponized,' What Should We Fear," John Herrman critiqued the

[7] Robert Jervis, *Perception and Misperception in International Politics.* Princeton, N.J. (Princeton University Press, 1976), 406.

modifier by avowing, “weaponization is used to describe both rhetoric that might incite violence and criticism of violent rhetoric…It is a shortcut to false equivalence, and it manufactures excuses for those with a vested interest in drawing blood themselves.”[8] According to Google Ngram Viewer, the use of the term “weaponize” has experienced exponential growth since 1990.[9] The widespread, nonchalant association of weaponization with conspiracy stories, fake news, federal funding, and political correctness heightens rhetoric for entertainment value or spurs unnecessary drama.[10]

The thoughtless associations with the term “weaponize” dilute a term best reserved for legitimate discussions about weapons of war and conflict. The use of the weaponize term began in the 1950s as military jargon to replace “to turn into a weapon” with an easily comprehensible and compact term that fit nicely in the realm of military operations.[11] Wernher von Braun, a former Nazi engineer who became an integral figure in the US space program, popularized its use when he linked his rocket propulsion work with the military’s ballistic missile technology and nuclear capabilities.[12] In this case, the term “weaponize” addressed the significance of changing the intended use of a capability to a weapon of war or deterrence.

## Section 2: Narrative in Context

Since the inception of societal groups, narratives—understood as the practice or art of telling stories—have been used to transfer history and knowledge. In larger groups, narratives were also used to justify or sway the aims and goals of political objectives. The strategic utility of narratives emerges “when they are not just stories, but when they draw on or create the frameworks from which societies, cultures, and individuals derive

[8] John Herrman, “If Everything Can Be ‘Weaponized,’ What Should We Fear?” *The New York Times*. March 14, 2017, sec. Magazine. https://www.nytimes.com/2017/03/14/magazine/if-everything-can-be-weaponized-what-should-we-fear.html.

[9]“Google Ngram Viewer.” Accessed April 20, 2018. https://books.google.com/ngrams/graph?content=weaponized&year_start=1900&year_end=2018&corpus=15&smoothing=3&share=&direct_url=t1%3B%2Cweaponized%3B%2Cc0.

[10] John Herrman, “If Everything Can Be ‘Weaponized.’”

[11] Ibid.

[12] Wernher von Braun had to cautiously manage his personal narrative. This narrative was “the peaceful scientist forced into a Faustian bargain to see his dreams of intergalactic travel come true.” There is belief that his core desire had always been to go into space, but different perceptions peg him as an opportunistic Nazi war criminal. Wernher von Braun had to distance himself from previous Nazi ties and the idea that his inventions were intended for military purposes rather than space exploration.

their identity and thus meaning—as consumers, as political actors, as individuals, as citizens."[13] Thus, truly effective narrative creates and guides the identities of individuals, groups, and nations.

A narrative's effectiveness in creating and guiding meaning is affected by the available media of communication at a given point in history. For example, while Martin Luther's nailed his 95 Theses on a church door in Wittenberg, Germany, his message traveled rapidly across the whole of Europe, with such dissemination made newly possible by Johannes Gutenberg's recently invented printing press. The printing press enabled narratives to influence a much wider audience at a dramatically faster pace. Written or spoken, verbal or non-verbal, a narrative is only limited by medium conduits. Narrative's job is to connect data with emotion to generate relative experience across the past, present, or future. This connection allows the extraction of meaning and the transfer of knowledge, information, or understanding, from which people build their identities and influence others. Narrative is continuously shaping human societies, acting simultaneously as a social-cultural bonding agent and a wedge.

## Section 3: Weaponized Narrative as a Strategy

Weaponized Narrative is a strategy. The three central components of Weaponized Narrative—namely intent/objective (ends), method (ways), and medium (means), as discussed earlier—align with the three key questions posed by Lykke's model: What is to be done? How is it to be done? What resources are required to do it in this manner?[14] According to Lykke, strategy is the resulting sum of ends, ways, and means. Lykke's theory does not provide a strategy. His paradigm conceptualizes valid strategy as the balancing of objectives, concepts, and resources.[15]

Combining Lykke's paradigm with Everett Dolman's definition of strategy provides additional insights on how an actor can leverage Weaponized Narrative as a strategy. In his book, *Pure Strategy*, Dolman defined strategy simply as "a plan for attaining continuing advantage."[16] Additionally, Dolman asserted that strategy "is an

[13] Braden Allenby, "The Age of Weaponized Narrative."

[14] H. Richard Yarger, "Towards A Theory of Strategy."

[15] Ibid.

[16] Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*. Cass Series--Strategy and History 6. London; New York: (Frank Cass, 2005), 6.

idea, a product of the imagination. It is about the future, and above all it is about change. It is anticipation of the probable and preparation for the possible."[17] Combining Dolman's ideas with the previous discussion on Lykke's paradigm and Weaponized Narrative, we arrive at the following idea: although the intent (ends) of Weaponized Narrative may not be achieved for decades, the media (means) and methods (ways) represent a plan for attaining continuing advantage.

The combined concept becomes clearer when remembering that Weaponized Narrative does not seek military victory, but rather the subversion of an adversary's institutions, identity, and/or will. That is, the true aim of a Weaponized Narrative strategy is "not so much to seek battle as to seek a strategic situation so advantageous that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this."[18] Weaponized Narrative does not seek cognitive clashes, but instead builds an advantageous situation by subverting an adversary by expanding schisms.

When an adversary leverages Weaponized Narrative, such actions are difficult to discern and visualize. The elusiveness of a Weaponized Narrative strategy is reflected in some of the earliest writing on the subject. Sun Zi suggested strategy should have "the highest standard in regard to dispositions (形, xing) is to have no discernible form (形, xing). When you have no visible form, even deeply embedded spies will be unable to see what is there and the wisest minds will be unable to devise a strategy against you."[19] The defender has the challenge of delineating existing schisms from new or exacerbated schisms. Furthermore, the defender must find a way to gauge, track, and protect identities and will, which mostly remain in the cognitive realm. Identification of such targeting efforts is all the more difficult for law enforcement and military members primarily trained in kinetic warfighting techniques, rather than cognitive conflict.

## The Clausewitzian Project

[17] Ibid., 1.
[18] B.H. Liddell Hart, *Strategy*. 2nd rev. ed. New York, N.Y., U.S.A.: Meridian, 1991, 325.
[19] Sun Zi, The *Art of War, Translated by Gary J. Bjorge*. Fort Leavenworth, KS, (Department of Military History, US Army Command and General Staff College, 2005), 62.

Another classic author on the subject of strategy, Carl von Clausewitz, asked how success in war “can be made more likely.” He concluded that two main ways exist: First, choosing objectives that directly bring about the enemy’s collapse—namely, destroying his forces and conquering his territory via violent military actions; and second, conducting operations with “direct political repercussions,” such as disrupting an adversary's alliances.[20] This thesis hereafter refers to efforts in the latter category as *Clausewitzian Projects*. Such projects may include actions that have direct political repercussions and actions that disrupt the opposing alliance or gain new allies.

Weaponized Narrative is a useful tool for executing such actions and fighting in the cognitive domain; that is, it provides a means to conduct *Clausewitzian Projects.* Ultimately, the enemy’s *will*[21] must be broken to achieve victory.[22] Clausewitzian Projects can affect *will* through cognitive force and therefore should not always be assumed as a support function for physical force. Paradigms that underestimate Clausewitzian Projects will restrict the development of strategy from exploring all available options to optimize effectiveness towards reaching political objectives.

Through the Clausewitzian Project—referring to a cognitive force or Weaponized Narrative in this thesis— shortcuts to achieving the political objective can be achieved without defeating the enemy’s forces.[23] Clausewitz says, “to think of these shortcuts as rare exceptions, or to minimize the difference they can make to the conduct of war, would be to underrate them.”[24] Cognitive force employed as a stand-alone operation, or supported minimally with physical force should be pursued as a valid road leading to success in war, conflict, or inter-state competition.

[20] Carl von Clausewitz, Michael Eliot Howard, and Peter Paret. *On War*. First paperback printing (Princeton, NJ: Princeton University Press, 1989), 92. Clausewitz described many roads leading to success in war; “they range from the destruction of the enemy's forces, the conquest of his territory, to a temporary occupation or invasion, to *projects* with an immediate political purpose, and finally to passively awaiting the enemy's attacks” (94).

[21] Will is a complex and nuanced phenomenon, some of which include concepts of mind, consciousness, cognition, creativity, psyche, spirit, transcendence, and soul.

[22] Clausewitz indicated that the enemy’s *will* is not broken until the enemy government and associated allies have been driven to ask for peace, or the population is made to submit. Carl von Clausewitz, *On War*, 90.

[23] Ibid., 92.

[24] Ibid., 94.

Strategy development is restricted if cognitive force is only viewed in supportive ways to physical force. One example of this mindset is the DoD term "Military Information Support Operations (MISO)," which encompasses other subordinate cognitive domain functions, namely, Information Operations, Psychological Operations, Military Deception, and Public Affairs. Inherent in MISO's name is the notion of support, which automatically places a cognitive force in subservient supportive roles in physical operations. Incidentally, strategists and planners often begin the formulation of strategy and operations with a narrow and limiting mindset of cognitive force.

A paradigm shift to increase the cognitive realm's relevance merits caution. Clausewitz gave warning that "kind-hearted people might of course think there was some ingenious way to disarm or defeat an enemy without too much bloodshed and might imagine this is the true goal of the art of war."[25] To be clear, nothing should be taken from the preparation and the development of capabilities to generate maximum physical force.[26] Underrating cognitive force, however, defensively exposes vulnerabilities to threats like Weaponized Narrative, and offensively limits the synergistic application of physical and cognitive forces to break an opponent's *will*.

Cognitive and physical forces share a common requirement to achieve a combat effective mindset. Clausewitz presented combat as the only means of war when he said, "however many forms combat takes, however far it may be removed from the brute discharge of hatred and enmity of a physical encounter, however many forces may intrude which themselves are not part of fighting, it is inherent in the very concept of war that everything that occurs must originally derive from combat."[27] The combat mindset may reveal itself in various ways, but the requirement exists alike for the infantryman who thrusts a knife in the belly of an opponent, an airman controlling an aircraft from a container on the opposite side of the globe, and the application of cognitive force.

[25] Ibid., 75.

[26] *Physical force* is the means of war that produces bloodshed, "for *moral force* has no existence save as expressed in the state and the law." Clausewitz, *On War*, 75. Clausewitz indicated that war "is a clash between major interests, which is resolved by bloodshed—that is the only way in which it differs from other conflicts" (149). Clausewitz's theory on war is "composed in equal parts of physical and of moral causes and effects. One might say that the physical seem little more than the wooden hilt, while the moral factors are the precious metal, the real weapon, the finely-honed blade" (184).

[27] Ibid., 95.

Cognitive warfare requires "considerable effort—the acme of skill—to subdue an enemy without [physical force]…by exercising reflexive[28] influence, almost parasympathetic control, over products of the adversary's neocortex."[29] The requirements of a combative mentality are restricted only by the attributes of actors and the spirit of the age, which determine the character of war.[30] Currently, the spirit of the age is exploring and expanding known boundaries to influence opponent's *will* in the cognitive domain.

### Section 4: Expanded Space for Conflict in the Cognitive Domain

Throughout most of history, warfare has involved competitive interactions between people using tools or machines to deliver violence against each other. This violence carried both a physical and a psychological aspect—impacting the will of an adversary to carry on a fight. What if an adversary can impact the psychological dimension without the threat or execution of physical violence?[31] In his article, "Neocortical Warfare? The Acme of Skill," Richard Szafranski argued that military power can increase in effectiveness even as it decreases in physical force because "military power resides in the domain of the mind and the will."[32] *Will* is brain-centered and therefore metaphysical control is the central aspiration of war or conflict.[33]

[28] For a detailed discussion of reflexive control see Timothy L. Thomas' article entitled, "Russia's Reflexive Control Theory and the Military."

[29] Richard Szafranski, "Neocortical Warfare? The Acme of Skill," in *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997), 395–416, 405. Szafranski said the acme of skill is attained when political objectives are met and the adversary voluntarily chooses the nonviolent alternative, potentially unaware of outside influence that led to the alternative decision reached.

[30] Clausewitz supported this notion when he said, "we can thus only say that the aims a belligerent adopts, and the resources he employs, must be governed by the particular characteristics of his own position; but they will also conform to the spirit of the age and to its general character." Clausewitz, *On War*, 594.

[31] The seminal works of *Arms and Influence*, by Thomas Schelling, and the *Dynamics of Coercion*, by Daniel Byman & Matthew Waxman, discusses the threat of physical violence through key concepts of coercion, deterrence, compellence, and brinksmanship.

[32] Richard Szafranski, "Neocortical Warfare? The Acme of Skill," in *In Athena's Camp: Preparing for Conflict in the Information Age*, 395–416. Szafranski stated that the neocortex is the capstone of the brain which "comprises 80 percent of total brain matter" …enabling us to "think, organize, remember, perceive, speak, choose, create, imagine and cope with or adapt to novelty."

[33] In the article, "Neocortical Warfare? The Acme of Skill," Richard Szafranski introduced a paradigm of Neocortical Warfare that "strives to control or shape the behavior of enemy organisms, but without destroying the organisms…Neocortical warfare uses language, images and information to assault the mind, hurt morale and change the *will*."

Arguably, belligerents operating in contemporary context have seen increased cognitive space in which to operate, for the expansion is changed by algorithms or machine intelligence—or more specifically, the increased faith people place in these tools for achieving their functional and emotional aspirations. The expanded cognitive space or gap is "the space between ideal and implemented computational systems, or between information and meaning…the tensions between computation and material reality."[34] The faith people place in algorithms creates exploitable space for conflict in the cognitive domain, with a host of new avenues for influencing institutions, identity, and/or will.

Algorithms bridge the gap between computational machines and human reality. Algorithms are evident everywhere, with significant new roles in the stock market, Netflix movie recommendations, Google searching, Facebook networking and news, to love connections on Match.com.[35] People rarely think about who is controlling the algorithm, about their motivations, or about potential long-term social impacts. For example, millions of people have joined Facebook or Instagram to connect with friends and family. In the background, sophisticated algorithms choose what advertisements and articles show up on an individual's page, interspersed among updates from friends and family. These algorithms can be changed at any given time, at the discretion of companies who can choose when, where, and if those changes are announced. These changes insidiously influence how people use the app and webpages, ever subtly steering people away from the reason they joined such programs. Algorithms are shaping humans, while simultaneously humans are shaping algorithms by the problems algorithms are asked to solve and by divulging large portions of human identities to pool in mass data.[36]

**Faith**

[34] Ed. Finn, *What Algorithms Want: Imagination in the Age of Computing*. (The MIT Press, 2017), 10.

[35] For further discussion of algorithms embedded in routine life see Ed Finn's book entitled, What Algorithms Want: Imagination in the Age of Computing.

[36] One example is the Cambridge Analytica scandal. See *The Washington Post* article entitled "Facebook suspends 200 apps following Cambridge Analytica scandal."

The faith people place in algorithms and advancing communication technologies expands the cognitive battleground.  Faith is the complete trust and confidence in something or someone even in the absence of acknowledgeable proof.  A useful analogy for digesting the concept of human faith in algorithms is the comparison with cathedrals, since "A cathedral is [both] a physical and a spiritual structure."[37]  These structures communicate a continual narrative, through relics, ceremonies, and weekly sermons; they present a gateway for collective belief, a framework to comprehend the world.[38]  Some portions remain hidden, with "schisms, budgets, scandals, doctrinal inconsistencies, and other elements of what a software engineer might call the 'back-end' of the cathedral are not part of the direct physical or spiritual façade presented to the world."[39]  Blind faith lets the "back-end" insidiously alter and take control of behavior, identity, and purpose. Extremist and radicals tend to grow from back-end issues because of blind faith and the lack of healthy questioning, debate, and reflection.

Replace the cathedral analogue with a company like Facebook, which has a structure in the form of apps and websites but has the same "back-end" issues that manifest in how Facebook manages algorithms.  People place their faith in in apps and websites but forget to consider the trajectory setting power of "back-end" considerations. Blind faith presents an expanded cognitive space of public governance, "(e.g., allowing Facebook users to promote particular causes through 'liking' them).  But their seemingly democratic interfaces are facades for the much deeper edifice of algorithmic arbitrage."[40]

Companies do not "often engage in overt censorship, but rather algorithmically curate the content they wish us to see, a process media scholar Ganaele Langlois terms 'the management of degrees of meaningfulness and the attribution of cultural value.'"[41] The result is companies use algorithms for the interest of profit and citizens use the same algorithms to fulfill personal desires.  Companies and citizens sometimes allow algorithms to lead in blind faith, presenting ripe conditions for cognitive exploitation and

[37] Ed. Finn, *What Algorithms Want*, 7.
[38] Ibid., 7.
[39] Ibid., 7.
[40] Ibid., 111.
[41] Ibid., 111.

conflict.  Blind human faith enables Weaponized Narrative to ride on the social interests of those using algorithms to further progress.

Opportunities for exploiting human faith in machine intelligence will expand through technological advancements such as brain-computer interfaces (BCIs).  BCIs place devices on the scalp or implants them into the brain to allow thoughts, information, or signal transfer in both incoming and outgoing directions.[42]  There are many skeptics, but using BCIs scientist have already circumvented paralysis, controlled monkeys by injecting data in their brains, and enabled around 150,000 people to help control Parkinson's disease.[43]  The literal definition of human may soon be challenged as BCIs advancement intermixes with human genetic engineering, wireless functions, the internet, and artificial intelligence.  Among many other potentials, the ability to distribute data and thoughts without prints, voice, or body language could mean another leap in the evolution of mass communication.  The implications are profound ranging from law, ethics, and healthcare, to the application in war and conflict.  The advantages of BCIs come with concerns about safety, privacy, and security.  Blind faith in BCIs will be inflammatory to cognitive vulnerabilities that Weaponized Narrative will be poised to exploit.

Another example of human faith being poured into machine intelligence is found in Matt Chessen's article, "The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy…and What Can Be Done About It."  In this article, Chessen discussed the most common type of machine intelligence used in computational propaganda known as

[42] In an adult human brain there are as many as 85 billion neurons each having 10,000 connections to other such cells.  Decoding neural activity opens remarkable possibilities and vulnerabilities. For example, the possibility of using decoded neural activity to control external devices, or the vulnerability of external devices controlling human brain activity.  For further discussion of BCI see the article "Brain-Computer Interfaces," *The Economist*, January 6, 2018.

[43] "Brain-Computer Interfaces." *The Economist*, January 6, 2018.  Other BCI aspirations include everything from Facebook's aspirations to deliver "thought-to-text typing" to the Elon Musk firm Neuralink, formed to upgrade humanity with the advent of artificial intelligence.  In 2018 the US Defense Advanced Research Projects Agency (DARPA) distributed $65 million to various organizations to create a high-resolution brain implantable interface.  The ideal implant would be safe, small, wireless, long-lasting, transmit huge amounts of data at high speed, and interact with more neurons than current technology allows.  The DARPA program has set an implant interaction target of 1 million neurons with a deadline of 2021 for a pilot trial in humans.

the web robot, or "bot."[44] One bot example he revealed is an artificial intelligence (AI) chatbot called Xiaoice, which is a Mandarin-language production of Microsoft. Xiaoice "is a special kind of bot[45] designed to engage in natural-language conversation with a human being."[46] What Microsoft personnel discovered in observing over twenty million registered users was that deep emotional connections were formed between users and Xiaoice.[47] Users professed to Xiaoice that "she" is the only available friend they have, some wish she could take human form as a girlfriend, and many tell Xiaoice that they love her. These desires of intimate emotional connections to algorithms or AI show just how much faith humans already have in machine intelligence. Blind human faith intertwined in advancing communication technologies expands cognitive battlegrounds and now enhances Weaponized Narrative's ability to steer, shape, and alter identities, institutions, and/or will.

## Bias

Algorithms and machine intelligence created enlarged cognitive space and deeper human-machine interactions; those interactions are vulnerable, exploitable, and susceptible to heuristics, bias, and error. Daniel Kahneman, in his book entitled, *Thinking, Fast and Slow*, explained these susceptibilities. He suggests human cognition functions via two simplified systems: System 1 performs the fast thinking, essentially functions automatically, and continuously generates suggestions for System 2.[48] System

[44] Chessen defines *computational propaganda* as a "new term for the use of social media, big data, autonomous agents, and related technologies for political manipulation. This can range from relatively benign amplification of political messages to insidious state-sponsored trolling and disinformation." Chessen then defines the term MADCOMs as "the integration of artificial intelligence systems into machine-driven communications tools for use in computational propaganda."

[45] Chessen said, emerging technologies are enabling AI chatbots to persuasively argue by analyzing vast amounts of knowledge, determining content in support of a position, and determining human emotional states from facial expressions and vocal patterns. Matt Chessen, "The MADCOM Future."

[46] Matt Chessen. "The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy...and What Can Be Done about It." September 29, 2017. https://weaponizednarrative.asu.edu/publications.

[47] Ibid.

[48] Daniel Kahneman, *Thinking, Fast and Slow*. 1st ed (New York: Farrar, Straus and Giroux, 2011), 20.

2 involves slow thinking, complex computations, choice, concentration, and monitors and controls System 1.[49] Of note, when these systems interact, "System 1 does not generate a warning signal when it becomes unreliable. There is no simple way for System 2 to distinguish between a skilled and a heuristic response. Its only recourse is to slow down and attempt to construct an answer on its own, which it is reluctant to do because it is indolent."[50]

The danger with algorithms and machine intelligence is that they provide a host of mental short-cuts and problem-solving functions in a System 1 fashion for humans. Arguably, humans are relinquishing System 2 functions of slow thinking, choice, and concentration to algorithms—and those algorithms are susceptible to bias, heuristics, and error. Moreover, an adversary who understands these limitations can manipulate human decision-making, identity, and ultimately *will*.

## Conclusion

Weaponized Narrative is the use of story-based communication to foment political and social schisms with the intent of subverting an adversaries' institutions, identities, and/or will. Narrative shapes societies and culture by connecting information, emotion, and identity. The shaping function acts as both a social-cultural bonding agent or a wedge. The term "Weaponized Narrative" increases awareness and understanding of narrative's wedge component, and the inclusion of the term in cognitive lexicon adds a new analytical tool to identify, communicate, and developing strategies for cognitive threats. Weaponized Narrative does this by compatibly merging with paradigms of strategy. Combining Lykke and Dolman's strategy paradigms with Weaponized Narrative, I arrived at the following idea: although the intent (ends) of Weaponized Narrative may not be achieved for decades, the methods (ways) and media (means) represent a plan for attaining continuing advantage.

A *Clausewitzian Project* is action that can have direct political repercussions, disrupt the opposing alliance, or gain new allies. The *Clausewitzian Project* encapsulates a way to view Weaponized Narrative as a cognitive force applied to influence the *will* of an adversary. *Will* resides in the human mind which is the target of all conflict and the

[49] Ibid., 21.
[50] Ibid., 416.

battleground for resolution.  The strategy of Weaponized Narrative has seemingly spiked in relevance as blind human faith is poured into advancing communication technologies. The public's growing blind faith in algorithms create an exploitable cognitive space susceptible to threats such as Weaponized Narrative.

# Chapter 3

## The Distinct Attributes of Weaponized Narrative

Weaponized Narrative is distinguished by unique qualities and characteristics that set it apart from other terms prominently referenced within the cognitive domain. Other terms within this domain include concepts like propaganda, cognitive hacking, and Military Information Support Operations (MISO), among others. Distinguishing Weaponized Narrative from these other terms and concepts will help strategists identify, communicate, and develop strategies that generate positions of advantage relative to adversaries.

This chapter begins by positioning Weaponized Narrative in contrast with the most prominent terms used within the cognitive domain. Definitions for these terms are provided, followed by comparative analysis that will illuminate similarities, differences, and exclusive traits. Then the common features of the changing information environment are presented that impact most cognitive domain terms.

### Predominant Terms in The Cognitive Domain

In comparison with the term Weaponized Narrative, I considered ten predominant cognitive terms. These terms hold in common that they each describe actions and efforts to influence various groups using the cognitive domain. I selected these ten terms by canvassing the relevant academic literature, along with military warfighting doctrine. Concepts common with the academic literature include propaganda, computational propaganda, disinformation, misinformation, command of the trend (weaponized social media), cognitive hacking, and themes or messages. Concepts common within military warfighting doctrine include MISO, information operations (IO), psychological operations (PSYOPs), military deception, and public affairs. The concepts of fake news, marketing, and public relations were not used in this study for two main reasons. First, fake news means different things to different people and is fraught with connotations of domestic policy. Second, the focus of this paper is external cognitive attack for the state, even though the techniques and tactics of marketing or public relations may overlap with cognitive domain terms. For the sake of brevity, prevailing definitions of each term are provided in Table 1; further explanations of each concept are available for reference in Appendix A.

**Table 1: Definitions of Cognitive Domain Terms**

**Weaponized Narrative:** Story-based communication to foment political and social schisms with the intent of subverting an adversaries' institutions, identities, and/or will.

**Propaganda / Computational Propaganda:** “Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.” (JP 3-13.2)

**Computational propaganda:** “is a new term for the use of social media, big data, autonomous agents, and related technologies for political manipulation.” (Chessen)

**Disinformation / Misinformation:** Disinformation is deliberately deceptive information, and misinformation is inaccurate information. Misinforming and disinforming are types of information behavior as the features below describe. (Karlova)

**Command of the Trend (Weaponized Social Media):** “Utilizing existing online networks in conjunction with automatic “bot” accounts, foreign agents can insert propaganda into a social media platform, create a trend, and rapidly disseminate the message faster and cheaper than through any other medium in history.” (Prier)

**Cognitive Hacking:** “Gaining access to or breaking into a computer information system to modify certain user behaviors in a way that violates the integrity of the entire user information system. Cognitive hacking can be either covert, which includes the subtle manipulation of perceptions and the blatant use of misleading information, or overt, which includes defacing or spoofing legitimate forms of communication to influence the user.” (Cybenko)

**Military Information Support Operations (MISO):** “Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives.” (JP 3-13.2)

**Information Operations (IO):** “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.” (JP 3-13)

**Psychological Operations (PSYOP):** “Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.” (JP 3-13.2)

**Military Deception:** "Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission." (JP 3-13.4)

**Public Affairs (PA):** "Communication activities with external and internal audiences." (JP 3-61)

**Theme / Message:** Webster Dictionary defines theme as "a subject or topic of discourse or of artistic representation."  JP 6-0 defines message as "any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication."  JP 3-61 describes a message as "a narrowly focused communication directed at a specific audience to support a specific theme."

*For expanded description and explanations of these terms see Appendix A.*

Source:  Author's original work derived from sources referenced above

### Comparative Analysis of Selected Cognitive Terms

While the respective works of literature on these 11 different cognitive domain terms are relatively extensive, few scholars compare them.  This chapter aims to address that gap by considering commonalities and differences among them.  Seven main categories (or characteristics) of comparison are considered here, including: 1) targeted audience (who); 2) the product (what); 3) sphere of utilization (when); 4) medium or forms of communication (where); 5) method of application (how), 6) objective or ends (why); and 7) the cognitive function (so what).

Each of these characteristics is explained below, followed by a description of how that characteristic might be measured or evaluated.  Then I compare the 11 respective cognitive terms under consideration to the specific characteristic.  The section concludes with a table that summarizes these differences and findings.  Analysis of said categories and the 11 cognitive domain terms will verify the distinct attributes of Weaponized Narrative, thus aiding strategists in identifying, communicating, and formulating strategy against threats in the cognitive domain.

Every tool within the cognitive domain has a *targeted audience*, a specific group of people that those using this tool hope to influence.  In simplest terms, the targeted audience can involve an internal audience or an external audience, an ally or an adversary.  Five of the eleven cognitive terms aim to influence only an adversary; this characteristic is shared by MISO, IO, PSYOP, military deception, and Weaponized Narrative.

Secondarily, *audience type* reflects the expected level of influence when using a cognitive term. The levels of influence range from individuals to selected groups to mass populations, or some variation along the spectrum. The use of Weaponized Narrative, command of the trend, and public affairs tend to permeate out to mass populations. Cognitive hacking is directed towards specific individuals, and military deception is primarily directed towards elite individuals. The remaining cognitive terms vary along the spectrum. Tracking the effects of cognitive terms are one challenge to accessing the targeted audience category.

The next category of *product* refers to the tangible (or sometimes intangible) manifestation of a given concept. The product can vary from a string of data, facts, and singular ideas to full-fledged stories or narratives. That information could be false, misleading, or exaggerated. For example, Weaponized Narrative and Public Affairs[1] distinctively share a story-based product focus, but this shared characteristic differs in one particular way—the story-based product of Public Affairs is predicated on truth, while Weaponized Narrative can be a conglomerate of true and false stories. This difference allows Weaponized Narrative to use an amalgam of products across the cognitive domain, whereas Public Affairs is restricted from using disinformation and cognitive hacking. Additionally, Public Affairs must be cautiously applied to retain credibility by spreading products seen as distinguished from false, misleading, or incorrect information components of propaganda, Command of the Trend[2], PSYOP, and military deception. The story-based composition of truth and falsehood found in Weaponized Narrative depends on the acceptable risk of those who command political objectives and end-states.

In the *utilization* category, there are two separate groupings: what societal groups primarily uses a cognitive term, and the expected period of intended effects when using a

[1] Public Affairs is the Department of Defense suborganization responsible for handling publicly disseminated information.

[2] See Table 1, above, for a definition of Command of the Trend. For a more in-depth description see "Command of the Trend: Social Media as a Weapon in the Information Age" written by Jarred Prier.

cognitive term.  Societal groups consist of private businesses, military branches, news media, politicians, and the general public.  In the US an observable divide exists for the cognitive lexicon used by the DoD.  MISO, IO, PSYOP, military deception, and public affairs primarily reside in DoD warfighting doctrine and culture, whereas the remaining cognitive terms are used across the spectrum of societal groups.

The DoD lexical divide aligns with a Western system of governance rooted in creating clear lines of delegation, responsibilities, and funding for DoD functions within society.  In contrast, clear lines of responsibilities are crossed and blurred when adversaries cognitively attack the US because America lacks a responsive lexicon to conceptually capture strategy in cognitive conflict.  The term “Weaponized Narrative” is a step towards communicating a shared understanding of cognitive attacks and formulating succinct responses across jurisdictions.

The effects or results of cognitive term application range in time from short-term to long-term.  Loose definitions—for this paper—of time periods are short-term (days to months), intermediate (months to 1-2 years), and long-term (a multitude of years).  Weaponized Narrative, MISO, IO, and Public Affairs predominately have a long-term focus despite short-term or intermediate effects obtained by using other cognitive terms within campaigns.  Outside of DoD-based cognitive lexicon, Weaponized Narrative is one of the few terms that naturally emphasize long-term effects—subverting institutions, identity, and/or will.  Unexpected realizations will occur while considering and dissecting the long-term implications posed by Weaponized Narrative.  US citizens far too often associate the stories of foreign cognitive influence with short-term or intermediate effects.

*Medium* is the places where the products of cognitive terms are found.  This broad category involves the full spectrum of verbal, written, and nonverbal communications, which are found in places like the internet, TV, radio, printed works, phones, music, and human interactions.  The ability to utilize all forms of communication is a similarity Weaponized Narrative shares with most other cognitive terms.  Some terms, however, are restricted to a particular medium, such as *command of the trend* and *cognitive hacking*, both of which occur only within internet networks.

**Table 2: Comparative Analysis of Cognitive Terms**

| | | Characteristics / Qualities | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | *Who (Targeted Audience)* | *Audience Type* | *What (product)* | *When (Used During)* | *When (Duration)* | *Where (Medium: Form of Communication)* | *How (Method)* | *Objective or Ends* | *Cognitive Function* |
| Cognitive Domain Terms | ***Weaponized Narrative*** | adversary | mass population | stories (true or false) | Anytime | Long-term | All | foment schisms | subvert institutions, identity, will or benefit sponsor | strategy (unrestricted) |
| | ***Propaganda or Computational Propaganda*** | adversary or ally | varies | facts & false, misleading or incorrect information | Anytime | Short-term | All | insert truth and falsehood | influence behavior or benefit sponsor | technique |
| | ***Disinformation or Misinformation*** | adversary or ally | varies | false, misleading, or incorrect information | Anytime | Varies | All | create falsehood | influence behavior, varies | tool |
| | ***Command of the Trend: Weaponized Social Media*** | adversary or ally | mass population | facts & false, misleading or incorrect information | Anytime | Short-term | Internet Networks | insert propaganda | shape behavior or benefit sponsor | technique |
| | ***Cognitive Hacking*** | adversary or ally | individual | false, misleading, or incorrect information | Anytime | Short-term | Internet Networks | insert falsehood | shape decision-making or benefit sponsor | technique |
| | ***Military Information Support Operations (MISO)*** | adversary | selected group | facts + false, misleading or incorrect information | DoD Operations | Long-term | All | alter emotions, motives, reasoning | influence behavior or benefit sponsor | concept |
| | ***Information Operations*** | adversary | selected group | facts + false, misleading or incorrect information | DoD Operations | Long-term | All | disrupt, corrupt, usurp behavior | influence decision-making or benefit sponsor | concept |
| | ***Psychological Operations (PSYOPs)*** | adversary | selected group | facts + false, misleading or incorrect information | DoD Operations | Intermediate | All | alter emotions, motives, reasoning | shape behavior or benefit sponsor | concept |
| | ***Military Deception*** | adversary | elites | facts + false, misleading or incorrect information | DoD Operations | Short-term | All | obscure truth | influence decision-making or support mission accomplishment | capability |
| | ***Public Affairs*** | adversary or ally | mass population | stories (true) | DoD Operations | Long-term | All | inform and educate population | shape behavior or support friendly creditability | strategy (restricted) |
| | ***Theme or Message*** | adversary or ally | varies | subject, thought, idea | Anytime | Varies | All | explain purpose of operations | shape behavior or benefit friendly forces | tool |

Source: Author's Original Work

The *method* category is the way or manner a cognitive term attempts achievement of its defined effects; the verbs used to describe a cognitive term usually reveal this. Most methods involve the creation or manipulation of truth and falsehood by varying the techniques of insertion, explanation, or obscuration. For example, MISO and PSYOP differ slightly by targeting emotions, motives, and reasoning, while Weaponized Narrative is distinct in that it explicitly aims to foment schisms between members of a given society. Distinguishing minor variations in methods are essential to achieving precision and clarity in the identification and communication of threats in the cognitive domain. Additionally, slight variations identified in the method category may reveal allusive intentions of opponents.

*Objective/ends* is a category that describes the goal of a tool used in the cognitive domain. Most cognitive tools aim at influencing and shaping behavior or decision-making to benefit the sponsor or to support mission accomplishment. The objective of Weaponized Narrative is distinct in that it aims at subverting institutions, identity, and will. Said differently, Weaponized Narrative can play for much higher stakes, and have significantly greater effects, when compared with objectives meant to merely change behavior. Subversion can range from destruction or destabilization to mild degrees of weakening or damage. Weaponized Narrative elevates awareness of elements within the cognitive domain that desire to weaken or destroy the existence of institutions and identity, rather than merely alter behaviors for momentary positional gains.

The last category of comparison is *cognitive function*, which expresses the application of a cognitive term in the cognitive domain. Tools, techniques, concepts, and strategies are the applications in the cognitive function category. Weaponized Narrative is distinctively an unrestricted strategy—unrestricted in what *products* can be used. By directing someone to conduct Weaponized Narrative against country X, that person would know to create stories (true or false) that foment schisms to reach the end-state of subverting an adversary to a certain degree. Public Affairs, in contrast, employs a restricted strategy that exclusively uses truth to target allies and adversaries with the objective of supporting allied credibility. The remaining cognitive terms serve as functional tools, techniques, or concepts.

Weaponized Narrative is directed towards adversaries (who) with effects permeating to mass populations.  It uses stories (what) consisting of truth and falsehood with a focus on long-term effects (when).  All forms of verbal and non-verbal communications (where) can be used to convey the stories found in Weaponized Narrative.  Fomenting schisms (how) is the method for achieving the subversion of institutions, identity and will (objective/ends).  Table 2 depicts the 11 cognitive terms analyzed using the seven comparative categories.  Weaponized Narrative is distinct as an unrestricted strategy (function) in the cognitive domain and provides unique attributes to bolster comprehension.  Furthermore, Weaponized Narrative adds greater severity to cognitive intentions, provides bridging across societal lexical divides, and draws attention to scrutinizing the long-term effects of unwanted foreign cognitive influence.

### Common Vulnerabilities and Opportunities for Cognitive Domain Terms

As discussed earlier, the 11 cognitive domain terms are united in their commonality of describing various actions and efforts used to influence people or groups using the cognitive domain.  How is the cognitive domain changing, given the proliferation of abundant, cheaply produced, readily available, and easily disseminated information of contemporary times?  To describe the challenges and opportunities within this rapidly changing information environment, practitioners like Anthony Olcott and Jon Hermann proposed two different models, known as Six Vs and V3S3, respectively.

Olcott and Hermann observed that the contemporary information environment has a remarkably low cost of entry, an overabundance of data, and ease of access and dissemination.  These influences are fundamentally changing the way humans allow information to alter deep-seated values, biases, and beliefs.  Information homophily is on the rise, meaning stronger horizontal bonds in ideology are made across national territorial borders, rather than vertical bonds to institutions and governments.  As a result, access is made more accessible for foreign influence to meddled in political and social schisms.  The features of the information environment are increasing the ability to tamper with human identities.

Olcott's Six Vs emphasize the massive amounts of almost incomprehensible information being produced in near real-time. The Six Vs include volume,[3] velocity,[4] vector,[5] veracity,[6] verifiability,[7] and vulgarity.[8] Indeed, elites have lost the monopoly of downward information flow to the masses; information now belongs to ordinary people who are "disrespectful of authority, hierarchy, and expertise."[9] Said differently, the ability of anyone to produce their own information and transmit their messages to the masses have neutralized the control of top-down information flow. Furthermore, the increased volume and velocity has intensified how much "information can be falsified, parodied, misdirected, easily blocked without the source of the block being obvious—or can be just plain wrong."[10] Jarred Prier summarizes Olcott's Six Vs in Table 3 (below).

[3] *Volume* refers to the vast amount information in production causing people to fend off information rather than fight to find information. Fending off information drives people towards homophily of interests to filter unwanted information with the assistance of a group. Anthony Olcott, "Institutions and Information: The Challenge of the Six Vs," ISD Working Paper in New Diplomacy, Georgetown University: Institute for the Study of Diplomacy, 2010.

[4] *Velocity* is the rate of information travel. Before the invention of the telegraph, information was restricted to the speed of the fastest animal or vehicle. Contrast with the present-day information age, when people expect instantaneous information if wanting to learn. Anthony Olcott, "Institutions and Information."

[5] *Vector* describes how information has diverged from predominately flowing downward from authorities and elites to masses. Downward information was a hallmark of power and control that was diluted by cheap means to distribute information. The masses are no longer reliant on authorities and elites for information. The result is "what 'everyone' believes, has become specific to the particular audiences, meaning that there is no longer a strong 'everyone.'" Anthony Olcott, "Institutions and Information."

[6] *Veracity* is the "vast increase in volume makes the issue of the truthfulness of information qualitatively more difficult than they were." Anthony Olcott, "Institutions and Information.

[7] *Verifiability* describes how information is more context-dependent than had been assumed by "Westerners in general, and Americans in particular, [who] are generally regarded as 'low context' information users, responding more to the content of information than to the manner in which it is conveyed (the speaker, the setting, and so forth). It is a widespread belief in the west that 'facts will speak for themselves.'" Context matters when attempting to prove or verify facts. Anthony Olcott, "Institutions and Information."

[8] "The new information environment is also 'vulgar' in the literal sense, that it belongs to ordinary people. This environment is massively disrespectful of authority, hierarchy, and expertise." Anthony Olcott, "Institutions and Information."

[9] Anthony Olcott, "Institutions and Information: The Challenge of the Six Vs." ISD Working Paper in New Diplomacy. Georgetown University: Institute for the Study of Diplomacy, 2010.

[10] Ibid.

**Table 3: Olcott's Six Vs**

| | |
|---|---|
| Volume | Massive amounts of information now produced and available on the internet. |
| Velocity | Information available in near real-time |
| Vector | Information no longer flows "downward, from authorities and elites to masses." |
| Veracity | Information may or may not be accurate |
| Verifiability | Source of information is difficult to prove |
| Vulgarity | From the Latin word "Vulgar," meaning from ordinary people. |

Source: Jarred Prier, "The Command of the Trend: Social Media as a Weapon in the Information Age" (SAASS Air University, 2017), http://www.dtic.mil/docs/citations/AD1039253.

In the article, "Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War," Jon Herrmann uses V3S3 to discuss the distinction between Weaponized Narrative from other cognitive domain terms. This study adjusted Herrmann's use of V3S3 to better describe changes in the cognitive domain which apply to most cognitive terms. Herrmann's V3S3 includes vector, vulnerability, virulence, scope, speed, and synergy (see Table 4). These concepts repeat or complement the ideas expressed by the Six Vs. He writes, "taken together [V3S3], a narrative can now deploy in a rapid-fire series of mutually-reinforcing stories that are hard for people to disregard and reach a global audience in seconds at minimal cost."[11] The essential additives—vulnerability, virulence, and synergy—express the susceptibility of the human mind in the progressive information environment. Precise sequential stories found in Weaponized Narrative can exploit the mind's hard to resist biases.[12] The table below (Table 4) provides a summary of Herrmann's V3S3.

[11] Jon Herrmann, "Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War." The Strategy Bridge, July 27, 2017. https://weaponizednarrative.asu.edu/publications/nine-links-chain.

[12] Ibid.

**Table 4: Herrmann's V3S3**

| | |
|---|---|
| Vector | Information is now self-propagating and has a global blast radius |
| Vulnerability | Sequential stories can overcome a mind's resistance |
| Virulence | Advanced understanding of cognitive flaws and heuristics empowers exploitation of biases |
| Scope | Information attacks can come from millions of sources in many combinations |
| Speed | Fire-hose rate of information that can be reinforced in seconds or minutes |
| Synergy | Each characteristic of the information environment discussed above is a force multiplier for the others |

Source: Jon Herrmann, "Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War." The Strategy Bridge, July 27, 2017.

## Conclusion

This chapter aimed to compare and contrast, as well as distinguish, Weaponized Narrative with respect to alternative cognitive domain terms. In contrast with the previous lexicon, Weaponized Narrative uniquely conveys the method of fomenting schisms and exacerbating social and political fissures in a long-term strategy, with the intended objective of subverting an adversary's institutions, identity, and/or will. In this regard, the 2018 Worldwide Threat Assessment of the US Intelligence Community states that influence operations,[13] "especially through cyber means, will remain a significant threat to US interests as they are low-cost, relatively low-risk, and deniable ways to retaliate against adversaries, to shape foreign perceptions, and to influence populations…. At a minimum, we expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople, and other means of influence to try to exacerbate

[13] Air Force Doctrine Document 2-5 defines influence operations as the employment of "capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle." "Influence Operations Ops, Propaganda, Deception, Counterpropaganda," Accessed April 20, 2018.

social and political fissures in the United States."[14] The use of Weaponized Narrative against the West is an attack against foundational principles of liberal democracy.

The distinct analytical additions provided by the term Weaponized Narrative contribute to how the US can categorically identify, precisely communicate, and enhance the formulation of strategy against the threat of cognitive influence. Undoubtedly, the features presented by the Six Vs and V3S3 will add complexity to the cognitive realm commensurate with the rapid pace of advancing communication technologies. Weaponized Narrative will not be the last addition or revision to the cognitive lexicon required as individuals and organizations continue to grapple in cognitive spaces.

[14] Daniel R. Coats, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. 2018, 11.

# Chapter 4

## Russian Weaponized Narrative during the 2016 US Presidential Election

> *Narrative provides and determines the meaning of events…events don't speak for themselves. Narratives speak for events.*
>
> Dr. Ajit Maan

The purpose of this chapter, and the next, is to examine how adversaries are using Weaponized Narratives. Both chapters aim at two principle objectives: 1) verifying the existence of Weaponized Narrative through tangible examples; and 2) increasing contextual understanding of how cognitive conflict manifests in the physical world. To aid in the first objective, the chapter leverages the previously proposed definition from Chapter 2, that Weaponized Narrative is *the use of story-based communication to foment political and social schisms with the intent of subverting an adversaries' institutions, identities, and/or will*. Attention is specifically drawn to the medium, method, and intent of Weaponized Narrative in the specific cases.

The second objective aligns with a central priority of the 2018 National Security Strategy (NSS), namely that Americans must understand "how adversaries gain informational and psychological advantages across all policies."[1] Once such advantages are understood, then one can move towards countering ideological threats, exposing adversary propaganda and disinformation, and effectively collaborating in communication campaigns.[2] The aim of defining Weaponized Narrative (previous chapters), and then examining its practical application using recent events (this chapter and the next), is to enhance future identification of cognitive threats and enable effective communication between government and private agencies tasked with formulating a strategy to counter them.

The event of interest in this chapter is Russia's influence operations and cognitive meddling in the 2016 US presidential election. The analysis will show the intent of Weaponized Narrative by presenting US perceptions of Russian influence activities and

[1] "National Security Strategy of the United States of America." US Government, December 2017.
[2] Ibid.

Russia's expressed desire for information operations in the US. The intent is extrapolated from Russian actions, stated desires, and US perceptions of Russian influence operations. Next, the media and methods of Weaponized Narrative are illustrated within Russian meddling during the 2016 US presidential election. The varying degree of Russian influence reinforce the goal of Weaponized Narrative and highlight the potential severity if the threat remains unchecked.

### The Intent of Weaponized Narrative: US Perception of Russian Influence

According to the proposed definition, when an actor uses Weaponized Narrative its ultimate intent is to subvert an adversary's institutions, identities, and/or will. Intent is difficult to discern, and judgments must be made when assessing and attributing intent. Once a judgment is made it should not be misconstrued as fact, but hopefully, a multitude of verifiable facts builds good judgment. The NSS interprets recent Russian influence operations as follows: "Russia uses information operations as part of its offensive cyber efforts to influence public opinion across the globe. Its influence campaigns blend covert intelligence operations and false online personas with state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"[3] In other words, cognitive attacks by Russia aim to exploit personal activities, interests, opinions, and values. As part of information statecraft, these attacks are designed to dismantle and invalidate the values and institutions that underpin free societies—to influence and shape the relationship between a government and the governed.[4] The US perception of Russian influence activity captured in the NSS implicitly refers to the intent defined in Weaponized Narrative.

The judgment of the 2017 US Intelligence Community Assessment similarly concludes that "Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[5]

[3] Ibid.

[4] Ibid.

[5] Intelligence Community Assessment, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution." January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Altogether, the US Intelligence Community (IC) and the NSS assessments conclude that the intended objective of Russian influence operations was to undermine public faith in the US democratic process. This shared conclusion matches the intent of Weaponized Narrative, and overt Russian claims validate US perceptions.

### The Intent of Weaponized Narrative: Russian Desired Effects

Russia's interest in the use of foreign influence operations for achieving political aims became evident in military writings by senior leaders. In 2013, for example, the Russian Federation Chief of the General Staff wrote, "the role of nonmilitary means of achieving political and strategic goals has grown and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[6] Just two years later in 2015, Sergey Chekinov, head of the Centre for Military Strategic Research of the Russian General Staff Academy, commented in a handbook addressing the content and nature of future wars:

> Wars will be resolved by a skillful combination of military, nonmilitary, and special nonviolent measures that will be put through by a variety of forms and methods and a blend of political, economic, informational, technological, and environmental measures, primarily by taking advantage of information superiority. Information warfare in the new conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, global computer networks (blogs, various social networks, and other resources).[7]

This quote suggests Russia is purposefully developing nonviolent means to take advantage of information superiority and revise the Russian paradigm of victory. Indirectly, information superiority can be forceful in a supportive role to violence or as a stand-alone main effort. The decisiveness of information superiority depends on the

[6] His statement was referencing the role of information warfare in the changing character of war, and he framed it as a response to Western use of narrative to promote the expansion of democracy and capitalism. See Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War." In Moscow's Shadows (blog), July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[7] Keir Giles, *Handbook of Russian Information Warfare*. NDC Fellowship Monograph Series; 9, Rome, Italy: NATO Defence College Research Division, 2016, 6. http://www.ndc.nato.int/download/downloads.php?icode=506.

political objectives pursued and the relative asymmetry of opponents.  Russian victory begins and ends in a state of peace where information warfare is conducted regularly and consistently.  War, too often defined in the West by physical death and destruction, begins and ends in the Russian conceptualization with a constant state of cognitive conflict or battle.  Therefore, Russia views cognitive force as a fellow peer of physical force; information warfare is adopted and blended into a whole-nation approach to warfare.

By 2016, Russians were connecting information warfare to the ability to subvert the US and restore parity lost to US conventional military dominance.  Russia held a national security conference called Info-Forum 2016. During this conference, Senior Kremlin Advisor Andrey Krutskikh said, "I'm warning you: We are at the verge of having 'something' in the information arena, which will allow us to talk to the Americans as equals."[8]  He continued by describing Russia's information warfare analogous to the Soviet testing of the atomic bomb in 1949, an act that enabled Russia to talk to Americans as equals.[9]

Information warfare is not a new concept, but the severity of its perceived effects is changing.  The perceived severity is demonstrated by Krutskikh's comparisons to Russia's development of atomic weapons—which secured nuclear parity with the US in 1949—coupled with direct cognitive threats against the US and the anticipation that these threats would be interpreted seriously.

The term Weaponized Narrative appropriately captures the Russian perceived severity and importance of information warfare.  In 1987, retired KGB General Oleg Kalugin explained the goal of active information warfare as driving "wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs."[10]  Said differently,

[8] David Ignatius, "Opinion | Russia's Radical New Strategy for Information Warfare." *Washington Post* (blog), January 18, 2017. https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.
[9] Ibid.
[10] The most common subcategory of active measures is *dezinformatsiya*, or disinformation: feverish, if believable lies cooked up by Moscow Centre and planted in friendly media outlets to make democratic nations look sinister.  Natasha Bertrand, "It looks like Russia hired internet

the US State Department simplified Kalugin's conceptual goal of information warfare with the verb *influence*.[11] The verb misses both the cognitive strategy that Kalugin describes and the severity change indicated by Krutskikh's claims of information warfare capabilities bestowing Russian parity with the US. Conversely, the term Weaponized Narrative captures the medium (friendly media outlets), the method (drive wedges and sow discord), and intent (weaken the US by painting democratic nations as sinister).

**The Method of Weaponized Narrative: Foment Schisms**

In February 2018, Robert Mueller, head of the US investigation of Russian interference, filed an indictment charging thirteen Russians and the Kremlin-linked Internet Research Agency (IRA) of "impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016."[12] The Russian method for influencing the 2016 US election was to widen and deepen preexisting divisions in America by weakening trust between the American media, the government, and the people.

One example is the polarized rhetoric between the administration of President Donald Trump, the FBI, and the news media. Each are now self-propelled in a spiral towards polarized division by the catalyst of Russian influence. President Trump tweeted on 17 February 2018, "if it was the GOAL of Russia to create discord, disruption and chaos…they have succeeded beyond their wildest dreams."[13]

The Russian influence campaign during the 2016 US presidential election exacerbated preexisting socio-political schisms between political parties, races, and religions. On example of fomenting schisms was the simultaneous release of derogatory information about several presidential candidates. Beginning in the first half of 2016,

trolls to pose as pro-Trump Americans." Business Insider, July 27, 2016.

[11] The US State Department reported the goal of Russian active information warfare was to "influence opinions and/or actions of individuals, governments, and/or publics." United States Department of State, "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 – 87," (Washington D.C.: Bureau of Public Affairs, 1987), viii.

[12] Robert Mueller, "Internet Research Agency Indictment." Department of Justice, February 16, 2018. https://www.justice.gov/file/1035477/download.

[13] Briefing: Russian Disinformation. "The Discord Amplifier: The Divided West Is Particularly Vulnerable to Russian Disinformation Campaigns, Whether Old-Fashioned or High-Tech." *The Economist,* February 24, 2018.

Russians choose to support the Donald Trump campaign while disparaging Hillary Clinton.[14] To accomplish these schemes, the Russians masked their identities, posed as US grassroots entities, compensated real US persons to promote or disparage, bought political advertisements, used social media, and staged political rallies.[15]

Around April 2014, the IRA expanded its operations on social media platforms including YouTube, Facebook, Instagram, and Twitter.[16] Shortly thereafter, the IRA integrated electoral interference into its strategy declaring the goal of "spread[ing] distrust towards the candidates and the political system in general."[17] By 2016 the IRA's monthly budget for influence operations was over $1.25 million, and the organization employed hundreds of personnel, with roles ranging from the creation of fictitious personas to administrative support.[18] These fictitious personas were used to drive public opinion—such as persuading US minority groups to vote for a third-party presidential candidate or not vote at all—and to shape the public narrative by accusing the Democratic Party of voter fraud.[19] Russian personnel were directed by the IRA to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements."[20]

Two examples illustrate how Russia used confusion and complexity to drive wedges in the populous during the American election process. Around June of 2016, the Russians promoted a rally called *Support Hillary; Save American Muslims*. Before the rally, the Russians advertised the event on a Facebook group called United Muslims of America. During the rally, Russian operatives recruited a US citizen to hold a sign with a quote of Clinton, "I think Sharia Law will be a powerful new direction of freedom."[21] After the rally, Russians posted on the Facebook group that Muslim voters were "between Hillary Clinton and a hard place."[22]

[14] Robert Mueller, "Internet Research Agency Indictment," 4.
[15] Ibid., 4.
[16] Ibid., 6.
[17] Ibid., 6.
[18] Ibid., 5, 7.
[19] Ibid, 18.
[20] As cited by Robert Mueller in "Internet Research Agency Indictment," 14.
[21] Robert Mueller, "Internet Research Agency Indictment," 21.
[22] Ibid., 21

A second example of Russia sowing confusion and complexity in the 2016 US election process occurred in November. The Russians organized and coordinated rallies that simultaneously supported president-elect Trump and protested the results of the election.[23] The same day in New York, Russians organized rallies called *show your support for President-Elect Donald Trump* and *Trump is NOT my President*.[24] Approximately a week later in Charlotte, North Carolina, Russians organized a rally called *Charlotte Against Trump* (see Figure 2, below).[25]

Both examples of Russian influence during the 2016 US election convey methods by which they fomented political schisms. Russia would praise and chastise candidates on both sides of the election race. Markedly, inflaming division was a higher priority than supporting a particular candidate. Any lopsided volume of praise and chastisement for either Trump or Clinton was to aggravate festering divisions.

| **2016 rallies planned and promoted by Russian Influence Campaign:** |
|---|
| Jun 25: March for Trump (New York) |
| Jul 9: Support Hillary. Save American Muslims (Washington, D.C.) |
| Jul 23: Down with Hillary (New York) |
| Aug 20: Florida Goes Trump (several Florida cities) |
| Oct 2: Miners for Trump (several Pennsylvania cities) |
| Nov 12: Show your support for President-Elect Donald Trump (New York) |
| Nov 12: Trump is NOT my President (New York) |
| Nov 19: Charlotte Against Trump (Charlotte) |

**Figure 2: US 2016 Rallies Planned by Russians**
Source: Alicia Parlapiano, "The Propaganda Tools Used by Russians to Influence the 2016 Election." *The New York Times*, February 16, 2018, sec. U.S.

Timing is essential to consider when attempting to identify the method of fomenting schisms. Figure 3, below, illustrates significant political events in the US and

[23] Ibid., 23.
[24] Ibid., 23.
[25] Ibid., 23.

Europe that correlate with the rise and fall of tweets per day by known Russian trolls. A noticeable increase in Russian tweet activity aligned with the declaration of President Trump as the Republican nominee in 2016. The tweet activity remained heightened until receding shortly after the 2017 inauguration. Events matched with timely social media activity became the means to reach significant numbers of Americans for purposes of interfering with the US political system.[26] Additionally, the 2016 rallies planned and promoted by Russian influence operations were placed intentionally in time and space to foment divisions (see Figure 3). Timing should factor into assessing the method and potentially the intent of Russian Weaponized Narrative.

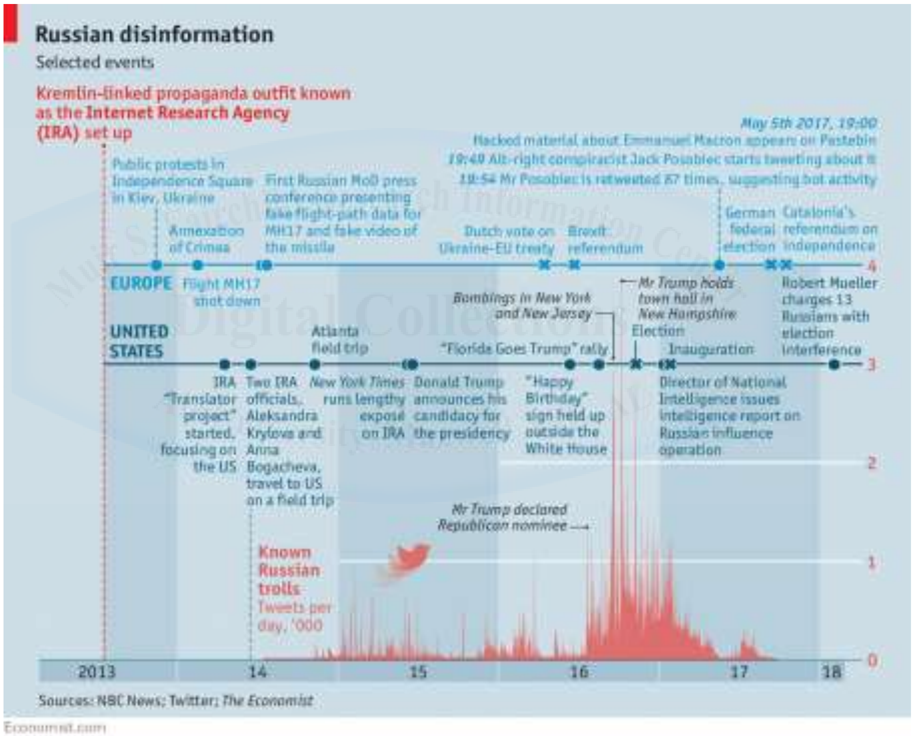


**Figure 3: Russian Disinformation Across Time**
Source: Russian Disinformation, "The Discord Amplifier," *The Economist*, Feb 24, 2018.

To summarize, Weaponized Narrative is evidenced by the adversary's efforts to foment socio-political schism. During the 2016 US presidential election, Russians played upon existing US political polarized oppositions, racial divides, and religious tensions.

[26] Robert Mueller, "Internet Research Agency Indictment," 3.

They did so by allocating resources to develop fake personas, exploiting social media and advertisements, and orchestrating political rallies. These actions used complexity and confusion, timed alongside critical electoral events to exacerbate American divisions and subvert US institutions.

### The Medium of Weaponized Narrative: Forms of Communication

Actors seek to deliver or enable a Weaponized Narrative via the use of various media such as TV, radio, prints, and the internet. In the Russian influence campaign, the full suite of communication media was used to create and instigate stories with mixtures of truth and falsehood. For example, cyberspace[27] enhanced Russian information operations by providing the means to: 1) conduct hacking to monitor and gather compromising information; 2) release or leak information; and 3) propagate messages, build followers, and exacerbate American divisions via social media. The results led to physical realities of Americans participating in Russian organized and coordinated rallies.

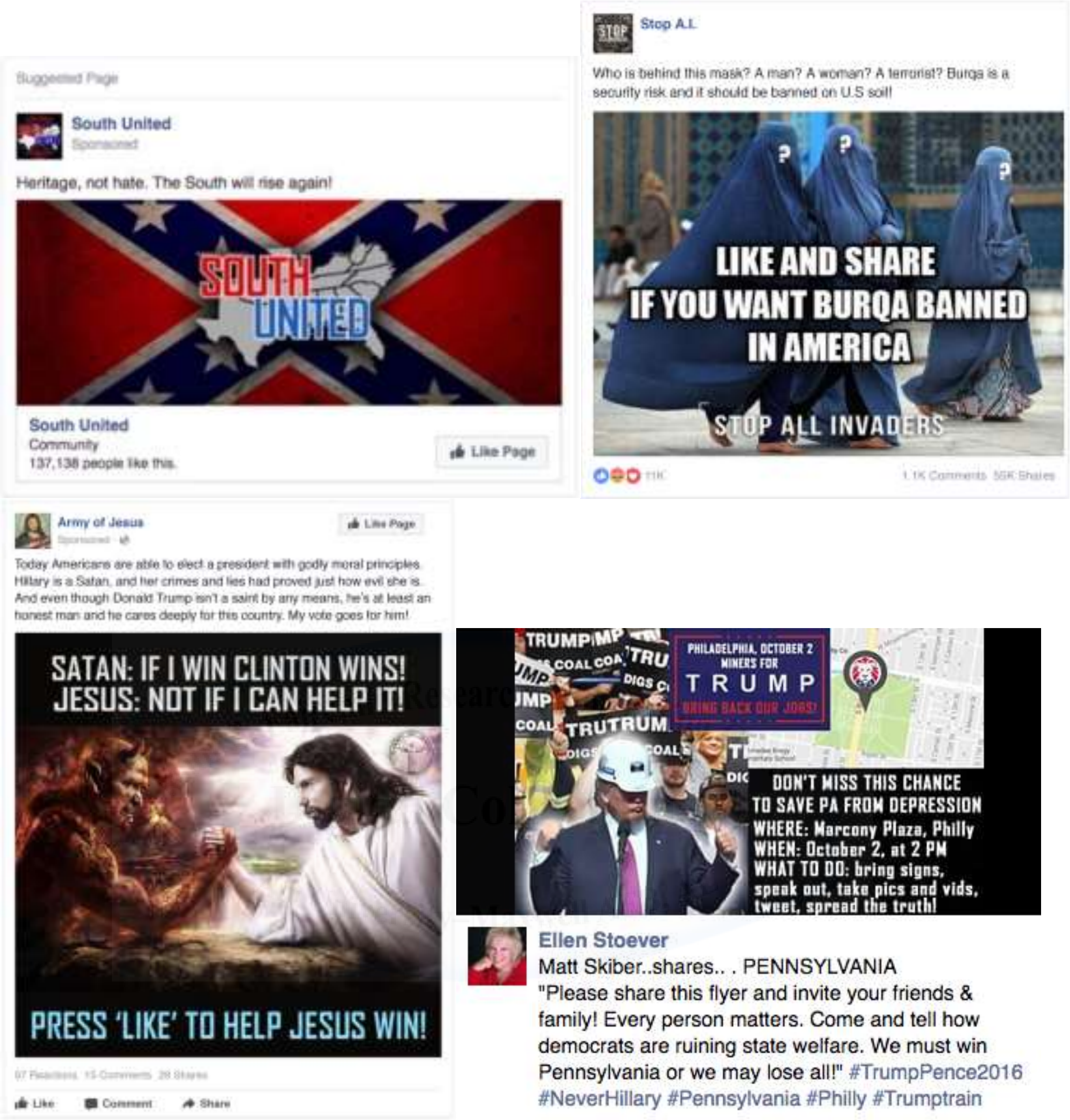
Indeed, the span of Russian influence achieved by social media is alarming, with many of their social media groups garnering more than 100,000 followers.[28] Congressional testimony in November 2017 verified that Russian electoral disinformation efforts reached a total of 146 million Americans (approximately 45% of the US population).[29] Facebook assessed that the IRA, the Russian-linked troll farm, was responsible for 120 fake pages and 80,000 posts.[30]

[27] Another example is the reality that *Russia Today (RT)*—a news media company with links to the Russian state--has content is on major TV networks in American homes and hotels across the US. Additionally, RT advertisements are readily apparent in newspapers, magazines, and airports. See Alexis Madrigal, "15 Things We Learned from the Internet Giants."

[28] Briefing: Russian Disinformation, "The Discord Amplifier," *The Economist*, Feb 24, 2018.

[29] Facebook accounted for 126 million people and Instagram accounted for 20 million. See Alexis Madrigal, "15 Things We Learned from the Internet Giants." Defense One. Accessed March 22, 2018. http://www.defenseone.com/politics/2017/11/15-things-we-learned-internet-giants/142279/. Mueller's indictment further confirmed that Facebook provides the principal avenue through which Russian agents sway Americans via "targeted political advertising and curated posts." Robert Mueller, "Internet Research Agency Indictment." Department of Justice, February 16, 2018. https://www.justice.gov/file/1035477/download.

[30] Special Report, "Waging War with Disinformation." *The Economist*, January 25, 2018. https://www.economist.com/news/special-report/21735479-power-fake-news-and-undue-influence-waging-war-disinformation.



Suggested Page

South United
Sponsored

Heritage, not hate. The South will rise again!

South United
Community
137,138 people like this.

Like Page

Stop A.I.

Who is behind this mask? A man? A woman? A terrorist? Burqa is a security risk and it should be banned on U.S soil!

11K 1.1K Comments 55K Shares

Army of Jesus
Sponsored

Like Page

Today Americans are able to elect a president with godly moral principles. Hillary is a Satan, and her crimes and lies had proved just how evil she is. And even though Donald Trump isn't a saint by any means, he's at least an honest man and he cares deeply for this country. My vote goes for him!

97 Reactions 15 Comments 28 Shares

Like Comment Share

Ellen Stoever
Matt Skiber..shares.. . PENNSYLVANIA
"Please share this flyer and invite your friends & family! Every person matters. Come and tell how democrats are ruining state welfare. We must win Pennsylvania or we may lose all!" #TrumpPence2016 #NeverHillary #Pennsylvania #Philly #Trumptrain

SOUTH UNITED
LIKE AND SHARE IF YOU WANT BURQA BANNED IN AMERICA
STOP ALL INVADERS
SATAN: IF I WIN CLINTON WINS!
JESUS: NOT IF I CAN HELP IT!
PRESS 'LIKE' TO HELP JESUS WIN!
PHILADELPHIA, OCTOBER 2
MINERS FOR
TRUMP
BRING BACK OUR JOBS!
DON'T MISS THIS CHANCE TO SAVE PA FROM DEPRESSION
WHERE: Marcony Plaza, Philly
WHEN: October 2, at 2 PM
WHAT TO DO: bring signs, speak out, take pics and vids, tweet, spread the truth!

**Figure 4: Russian Propaganda Tools Used During the 2016 US Presidential Election**
Source: Alicia Parlapiano, "The Propaganda Tools Used by Russians to Influence the 2016 Election." *The New York Times*, February 16, 2018, sec. U.S. https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html.

The Russians demonstrated an understanding of Facebook algorithms by focusing advertising on increasing followership and then distributing their content organically. Figure 4, above, displays samples of Russian propaganda tools used to target preexisting race, religion, and political rifts in the US.[31] Russian algorithm understanding did not happen by chance. Beginning at least in 2014, the IRA tracked and studied socio-political groups on US social media sites by observing metrics such as group's size, the frequency of posted content, and audience engagement (average number of comments or responses to a post).[32] Facebook reported 3.3 million Americans directly following Russian pages, but the details became vague when attempting to answer who precisely was following the pages.[33] Algorithms failed to filter the intent to foment American schisms.

## Conclusion

The term Weaponized Narrative—and its definition in this thesis—provide a new conceptual framework for analyzing and understanding cognitive schemes used by adversaries. This chapter demonstrated, for example, how Russian influence operations during the 2016 US presidential election exhibited the intent, method, and media defined by Weaponized Narrative. The assessments of the US Intelligence Community and the NSS combined with Russian expressed interest in cognitive influence operations confirm the *intent* of Weaponized Narrative. The *method* was established by demonstrating Russia's schemes to exacerbated preexisting socio-political schisms between political parties, races, and religions. Finally, cyberspace proved to be a pivotal *medium* to deliver the products necessary to foment schisms. The next chapter will show the effects of Russian Weaponized Narrative as an overarching effort persistent before, during, and after the 2016 US election.

[31] For a list of Russian advertisement themes in the US presidential election from April through October, 2016 see page 20 of Robert Mueller's "Internet Research Agency Indictment."

[32] Robert Mueller, "Internet Research Agency Indictment," 12. Further exploitation of algorithms occurred when *Russia Today (RT),* a news media company with links to the Russian state, qualified for YouTube's preferred advertising program. See Alexis Madrigal, "15 Things We Learned from the Internet Giants."

[33] Alexis Madrigal, "15 Things We Learned from the Internet Giants."

# Chapter 5

## Russian Weaponized Narrative Beyond the 2016 US Presidential Election

Analysts attribute Russian meddling in the election to the following result: a US president sympathetic towards Russia. Subversion—the objective of Weaponized Narrative—may get overlooked by not challenging seemingly apparent motives. Fomenting schisms by injecting complexity and confusion can be done for no other reason than to degrade, undermine, or destroy US socio-political systems. Dan Mahaffee, the Senior Vice President at the Center for the Study of the Presidency & Congress, discussed the need to look past surface-level motives:

> For Russian President Vladimir Putin, the main goal is steady degradation of U.S. electoral processes and the tenor of our politics. Whether a specific candidate wins is less important than sowing doubt about the legitimacy of our elections in the minds of both the American people and those overseas who look to American democracy as a model. The Russian campaign includes not only efforts to hack voting machines and electoral rolls, but also the seeding of divisive issues through social media. To counter this insidious campaign, we must understand the underlying motives and methods of our adversary.[1]

The short case studies referenced in this chapter demonstrate Russian efforts to subvert the US beyond its involvement in the 2016 US election. This chapter argues that Russia has deeper motives—beyond US candidate preference—to subvert US democratic society by cognitively attacking the minds of the US public. The cases investigated in this chapter discuss the 2014 Louisiana and Atlanta hoaxes, racial divisions, religious disunions, and the Parkland High School shooting in Florida. Conceptualized these cases with Weaponized Narrative will prove that Russia's goal to subvert American democracy supersedes any desire to sway victory for a specific candidate in US elections.

[1] Dan Mahaffee, "We've Lost the Opening Info Battle against Russia; Let's Not Lose the War." Defense One, Accessed March 25, 2018. http://www.defenseone.com/ideas/2018/02/weve-lost-opening-info-battle-against-russia-lets-not-lose-war/146212/.

## 2014 Louisiana and Atlanta Hoaxes: #ColumbianChemicals, #EbolaInAtlanta and #ShockingMurderInAtlanta

On September 11, 2014, the town of St. Mary Parish, Louisiana, fell victim to a Russian-induced hoax. A fake story spread that a local chemical plant exploded resulting in a fire and the release of harmful toxic fumes that now threatened the town. The story spread quickly via multiple communication media, including text messages, social media, and even the local news. Panic and chaos ensued for a two-hour period before an official report was released stating reports of the explosion were false.

While some considered the hoax as a simple and a rather tasteless prank performed on the anniversary of September 11th, an alternative view is that this event reveals the deeper motives and potential dangers of Weaponized Narrative. From this perspective, the two-hour block of chaos and confusion was a well-orchestrated influence operation. The Russians had to coordinate multiple fake social media accounts, hundreds of tweets or posts, and text messages sent to local individuals. Furthermore, the Russians created customized YouTube videos of explosions and rising smoke, all linked to a specially created Wikipedia page designed for the fake chemical plant disaster. Fabrication even included "fully functional clones of the websites of Louisiana TV stations and newspapers."[2] The hoax was so well executed that dozens of journalists, news media outlets, and politicians, ranging from Louisiana to New York City, were inundated with messages from those who believed the explosion to be real.[3]

On December 13, 2014, the Russian IRA was responsible for two additional Weaponized Narrative attacks carried out with the same depth and detail of the Louisiana chemical plant hoax. The first fake story reported a fresh outbreak of Ebola in Atlanta, Georgia just two months after a handful of actual Ebola cases occurred in the US.[4] The second fake story, released on the same day, was that "an unarmed black woman had been shot to death by police."[5] This story similarly capitalized on previous historical

[2] Adrian Chen, "The Agency," The New York Times, June 2, 2015, sec. Magazine, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[3] Ibid.

[4] Ibid.

[5] Ibid.

events and sensitivities, namely the proceeding summer and fall protest that year over the shooting of Michael Brown (a black male) in Ferguson, Missouri.[6]

The effects of Russian Weaponized Narrative go well beyond juvenile pranks. For example, both of the Atlanta hoaxes created false stories designed to piggyback on recent truthful events. Piggybacking made public acceptance more likely and improved the probability of success in aggravating societal divisions and anxieties. Seeds of doubt were planted in the public mind about what measures of environmental safety actually existed, whether or not the news media, local government institutions, and local businesses ought to be trusted, and whether the government is capable of keeping Russia out of sensitive internal US affairs. The hoaxes also afforded Russia the opportunity to conduct social network analysis as they injected falsehood and confusion into America. They could gather, for example, valuable data on response times and institutional reactions. These insights help as Russia plans out future exploitation.

### Racial Divisions: 2015 #PrayforMizzou, 2016 # BlackLivesMatter

Russian attempts to influence racial tensions in America are not new. Their efforts were evident during the civil rights movement led by Martin Luther King Jr. in the 1960s all the way to the present-day Black Lives Matter activities. What has changed in the current era is internet availability, which enables greater reach with less human-to-human contact.

During the Cold War era, the Soviets employed a variety of activities all aimed at subverting American democracy by exacerbating racial tensions. For example, the Soviets "concocted the story that HIV and AIDS were developed by the CIA as a bio-weapon as a way to keep down nonwhites."[7] In 1984, the Soviets forged letters from the Ku Klux Klan (KKK) in an attempt to scare Africans and Asians from participating in the Summer Olympics.[8] Soviets schemes also included fake leaks of presidential memorandums and the pitting of black activists against Zionist Jewish groups. The KGB

[6] Ibid.
[7] Philip Ewing, "Russians Targeted U.S. Racial Divisions Long Before 2016 And Black Lives Matter." NPR.org. Accessed March 26, 2018. https://www.npr.org/2017/10/30/560042987/russians-targeted-u-s-racial-divisions-long-before-2016-and-black-lives-matter.
[8] Ibid.

solicited Dr. King for an internal political insurgency against the US. After Dr. King refused, the KGB tried to undermine him.[9]

On November 11, 2015, the Russians manipulated the hashtag #PrayforMizzou to exacerbate racial tension. The hashtag initially resulted from protests over racial issues at the University of Missouri campus. Russians shaped and steered the resulting dialogue on Twitter and elsewhere, with fake messages portraying cops marching with the KKK and tweets describing shootings, stabbings, and cross-burnings that had not occurred.[10] Thousands of messages were retweeted from this stream, generating outrage across the US. Locals retreated to shelter in fear and journalists hit the streets searching for marching KKK groups that did not exist. The Russian hoax successfully created a flurry of fear, outrage, media coverage, and tension using fake events that never occurred, but that seemed similar enough to previous events that few initially questioned their veracity. A real concern of this Russian influence, voiced well by Representative Cedric Richmond, chairman of the Congressional Black Caucus, is that they cause undue, misplaced "harm and additional resentment to young people who unselfishly fight for justice and equality for African Americans and other marginalized communities."[11]

Russia continued instigating racial divides in America during the 2016 US election period. When National Football League (NFL) players protested for the oppressed people of color by kneeling during the national anthem, Russian Twitter accounts agitated both pro-player and anti-player sides of the controversy. On Facebook, the Russians used an account called *Blacktivist*, which led calls to action for African Americans to "wake up and fight mass incarceration and death of black men."[12] On the other side of the racial divide, and after the US election, Russian social media bots

[9] King was one of the few prominent Americans to be the target of active measures by both the FBI and the KGB. The FBI, under then-Director J. Edgar Hoover, "ran a campaign to hound King in 1964, including with listening devices in his hotel and letters threatening to ruin him. Distrust endures to this day between black leaders and the FBI." Philip Ewing, "Russians Targeted U.S. Racial Divisions."

[10] Jarred Prier, "The Command of the Trend: Social Media as a Weapon in the Information Age," SAASS Air University, 2017, 49. http://www.dtic.mil/docs/citations/AD1039253.

[11] Philip Ewing. "Russians Targeted U.S. Racial Divisions Long Before 2016 And Black Lives Matter." NPR.org. Accessed March 26, 2018. https://www.npr.org/2017/10/30/560042987/russians-targeted-u-s-racial-divisions-long-before-2016-and-black-lives-matter.

[12] Philip Ewing, "Russians Targeted U.S. Racial Divisions."

bolstered supportive messages for a white supremacist rally held on May 13, 2017, in the town of Charlottesville, North Caroline. Russia continues to learn how it can manipulate different media in ways that exploit vulnerabilities in American democratic institutions and preexisting social schisms.

### Religious Division: Hearts of Texas and United Muslims of America

On May 21, 2016, Russia demonstrated the ability to use Weaponized Narrative in a way that successfully incited two opposing societal groups to meet up at the same time and place in protest against the other. The hoax was carried out between two Russian-created Facebook groups named *Heart of Texas* and *United Muslims of America*. The two Russian Facebook sites were each able to generate more than 250,000 followers.[13] Next, Russia advertised on both Facebook sites that a protest would be held outside a Houston mosque; the protests were scheduled for the same day and time.[14] On the *Heart of Texas* site, Russia promoted "Stop Islamization of Texas," while on the *United Muslims of America* site Russia posted "Save Islamic Knowledge" (see Figure 5, below). The result was that the Russians successfully pitted Americans against other Americans in an angry but non-violent protest, all orchestrated from St Petersburg, Russia, at the cost of less than $200.[15]

[13] Ryan Lucas, "How Russia Used Facebook To Organize 2 Sets of Protesters." NPR.org. Accessed December 20, 2017. https://www.npr.org/2017/11/01/561427876/how-russia-used-facebook-to-organize-two-sets-of-protesters.

[14] Ibid.

[15] Ibid.

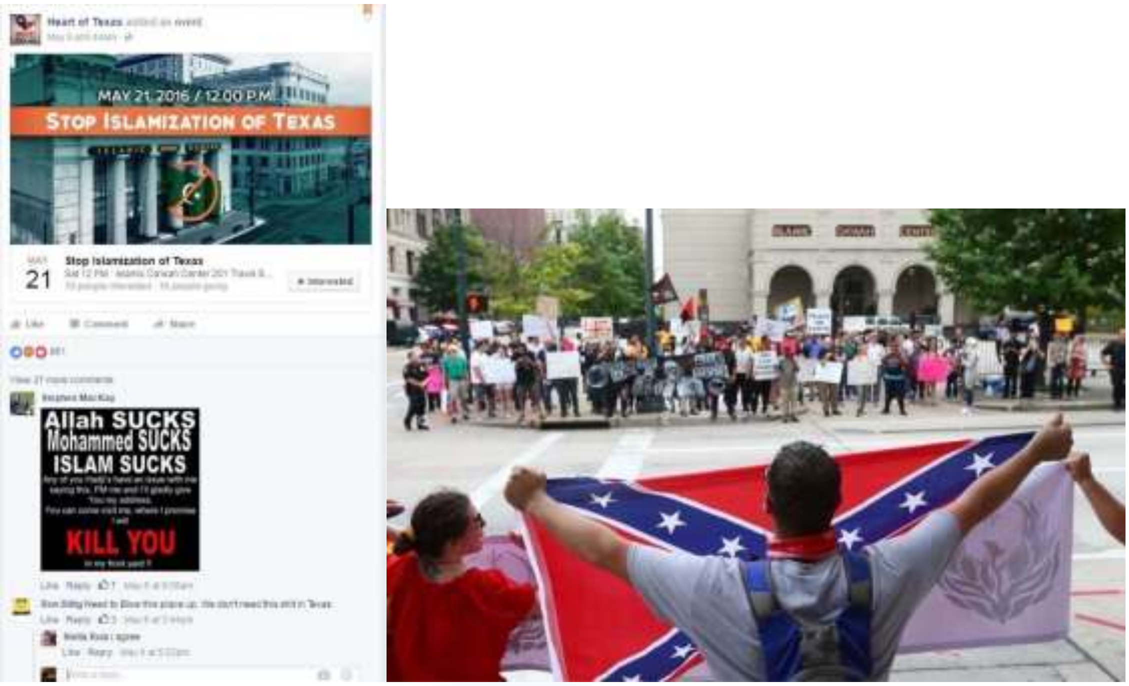


**Figure 5: Protest Street View of Hearts of Texas and United Muslims of America**
Source: Mike Glenn, "A Houston Protest, Organized by Russian Trolls." Houston Chronicle, February 20, 2018. https://www.houstonchronicle.com/local/gray-matters/article/A-Houston-protest-organized-by-Russian-trolls-12625481.php.

### Russian's Contemporary Use of Weaponized Narratives

Russia's efforts to agitate socio-political divisions continues today, with actions evident in US politics, general racial issues, immigration, and recently, gun control. On February 14, 2018, just one hour after the high school shooting in Parkland, Florida—in which 14 students and three staff were murdered—Russian social media accounts rapidly kindled a renewed gun control debate. The accounts used the hashtags #guncontrolnow, #gunreformnow, and #parklandshooting, while simultaneously posting to hashtags from the opposite perspective, such as #ar15 and #NRA. Earlier that same day, the Russian accounts were focused on the Robert Mueller investigation into Russian meddling in the 2016 US presidential election.[16] Only two days later, the Russia accounts moved on to the hashtag #falseflag—an intelligence term referring to secret government operations

[16] Sheera Frenkel, "After Florida School Shooting, Russian 'Bot' Army Pounced." *The New York Times*, sec. Technology, Accessed March 27, 2018. https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html.

executed in a manner designed to misattribute responsibility for the events. The Russian claim was that the Parkland shooting was a conspiracy theory that never happened.

According to Jonathon Morgan, chief executive of New Knowledge, a company that tracks online disinformation campaigns, "the [Russian] bots focus on anything that is divisive for Americans. Almost systematically."[17] The bots to which Morgan refers are Twitter bots aimed at heightening frustration and anger via any division they can find in America. Karen North, a social media professor at the University of Southern California, said the bots are intentionally designed to search out contentious and divisive issues with the aim of making the issue ever more indivisible, frustrating, and vexing for the involved parties.[18] By day five, Russian bots shifted from the Parkland shooting back to the 2018 midterm elections, an obvious irresistible target for bots and Weaponized Narrative.

## Conclusion

The short episodes outlined in this chapter are more than silly hoaxes. They represent well-planned, well-resourced, elaborate, and persistent long-term strategies by Russia to undermine the US. Russia's actions, however, are not limited to the US alone. Abroad, Russia has also used Weaponized Narratives against Estonia in 2007, Ukraine in 2014, France in its 2017 presidential election, and NATO and BREXIT (ongoing). Furthermore, Russia's efforts are not merely about shaping or influencing behavior for short-term benefit. Instead, as US Senator Mark Warner (D-VA), the vice chairman of the Senate Select Committee on Intelligence, stated in a February 2018 hearing on global threats to the US, "what we're seeing is a continuous assault by Russia to target and undermine our democratic institutions, and they're going to keep coming at us."[19]

We see an adversary who understands that narratives shape, mold, and influence how people interpret and react to contemporary events. By using the term Weaponized Narrative to evaluate these actions, strategists can tangibly identify the media, method, and intent and communicate such actions more clearly to policymakers and the population. Moreover, this terminology corrects a critical gap in the current lexicon—one that is constrained to more limited cognitive terms like disinformation campaign,

[17] Ibid.
[18] Ibid.
[19] Ibid.

influence campaign, propaganda, and meddling, alongside the other cognitive domain terms discussed in Chapter 3.

Information warfare and Weaponized Narratives are creative asymmetric ways to subvert the US, liberal democracy, and Western alliances.  Future studies might evaluate how China has used Weaponized Narrative to achieve geopolitical objectives in the South China Seas and how violent extremist organizations have leveraged narratives as means for mobilizing and motivating non-state actors into violent action.  See Appendix B for this study's brief initial analysis of Weaponized Narrative used by China and ISIS.

# Chapter 6

# International Relations

Do the cases of Russian influence in the US cognitive domain matter in relative international state power? This chapter addresses why a state would have respectable concern with Weaponized Narrative and sets it within the context of international relations between states. Three specific applications are considered, including: 1) the impact of Weaponized Narrative on state power, specifically with respect to how that state can wield hard and soft power; 2) ambiguity in international law; and 3) the unique challenges that democracies face in responding to events where Weaponized Narrative was used against them.

The discussion will demonstrate that Weaponized Narrative is a form of sharp power that works by manipulation and pressure. Sharp power stops well short of hard power (military or economic force), but it more malign and distinct from the soft power attraction of culture and values.[1] Furthermore, the chapter will show that Weaponized Narrative strategies are attractive because of ambiguity in the international law and behavioral norms. Finally, the chapter will reveal that democracies have unique challenges defending and developing deterrence strategies to thwart Weaponized Narrative aggression.

## Weaponized Narrative Wields Power

Weaponized Narrative is a type of *sharp* power capable of degrading the relative *hard*, *soft*, and *smart* powers of actors in the international community. Defining of these terms is necessary to grapple with what this declaratory statement means. Power, defined as the "ability to influence outcomes in a desired direction," is a complicated and nuanced phenomenon.[2] Ranging from the state to individual levels, power encompassed the ability to impose will by force called *hard* power (to push), a charismatic appeal authority eliciting positive attraction called *soft* power (to pull), or a combination of both

[1] Briefing: China and the West, "At the Sharp End," *The Economist*, December 16, 2017.

[2] Michael Sheehan, *The International Politics of Space (Space Power and Politics)*. 1 edition. London; New York: Routledge, 2007, 20

called *smart* power.  Hard power includes tangible factors such as force and money, while soft power includes intangible factors such as "institutions, ideas, values, culture, and the perceived legitimacy of policies."[3] The delineation between hard and soft power becomes murky with intangible factors such as patriotism, morale, and legitimacy, which would be categorized as soft power but affect aspects of hard power.[4]

In contrast to hard and soft power, Weaponized Narrative is a form of *sharp* power.  The definition of sharp power is to "pierce, penetrate, or perforate the information environments in the targeted countries."[5] To enumerate, sharp power seeks to "subvert politics, media and academia, surreptitiously promoting a positive image of the country [employing sharp power], and misrepresenting and distorting information to suppress dissent and debate."[6] Indeed, sharp power enables authoritarians to cut, razor-like, into the fabric of society, stoking and amplifying existing divisions.  Cash-strapped universities, human blind faith in algorithms, and global connectedness are the principal avenues by which an actor can pierce, perforate, and penetrate a society.  Unlike the blunt impact of hard power or the gaudy magnetic pull of soft power, sharp power entails a degree of stealth.[7] In summary, sharp power is the ability to influence a targeted audience by the pressure of manipulating or poisoning the information environment of the targeted country.

The twenty-first century has witnessed the diffusion of power away from the state as the principal controller of information.  What dangers exist when a state loses power and control over the key narratives in that state?  A state acts based on national identity, beliefs, and its understanding of reality.  In this vein, Joseph S. Nye Jr. concluded that a country like the US would potentially "decline in terms of relative power not because of imperial overstretch, but because of *domestic underreach*.  As historians remind us, Rome rotted from within.  *People lost confidence in their culture and institutions, elites*

[3] Joseph S. Nye Jr. *The Future of Power*. New York: Public Affairs, 2011, 21.
[4] Ibid., 21.
[5] Juan Pablo Cardenal, Jacek Kucharczyk, Grigorij Mesežnikov, Gabriela Pleschová, Christopher Walker, and Jessica Ludwig. *Sharp Power: Rising Authoritarian Influence*. National Endowment for Democracy, 2017, 13.
[6] Briefing: China and the West, "At the Sharp End," *The Economist*, December 16, 2017.
[7] Juan Pablo Cardenal, Jacek Kucharczyk, Grigorij Mesežnikov, Gabriela Pleschová, Christopher Walker, and Jessica Ludwig. *Sharp Power: Rising Authoritarian Influence*. National Endowment for Democracy, 2017, 13.

*battled for control*, corruption increased, and the economy failed to grow adequately."[8] The US is not impervious to the internal rot experienced by the Roman Empire. Dominant narratives help to shape a perceived reality, and if foreign actors want to influence an opponent's internal realities, then Weaponized Narrative is a potent, penetrating strategy that might lead to such domestic underreach, to socio-political divides and loss of confidence in a uniting culture and corresponding institutions.

Politics in the information age is a contest of credibility, and ultimately about whose story wins in the quest to the control narrative. Nye equates narrative as the currency of soft power.[9] So, if narrative is the currency of soft power, then Weaponized Narrative is the devaluation of that currency, a plummeting in the exchange rate of soft power. In other words, Weaponized Narrative attacks the three basic resources of soft power, namely: "*its culture*[10] (in places where it is attractive to others), *its political values* (when it lives up to them at home and abroad), and *its foreign policies* (when others see them as legitimate and having moral authority."[11] The ability to penetrate and exacerbate political and social schisms is a sharp power which acts as a counterforce to soft power. The target for soft and sharp power is the broad public opinion and cultural attitudes.[12] Soft power—being the city upon a hill[13]—requires consistency of actions aligned with values.[14] Sharp power or Weaponized Narrative derails the alignment of actions and values or builds a perception of misalignment.

Military and economic hard powers are often accredited as the most important forms of power in world politics. Guns and sanctions, however, are not always the best approach to promoting democracy, liberal economies, and human rights. Exacerbated

[8] Emphasis mine. See Joseph S. Nye Jr. *The Future of Power,* 187.
[9] Joseph S. Nye Jr. *The Future of Power*, 104.
[10] "Culture is the pattern of social behaviors by which groups transmit knowledge and values, and it exists at multiple levels. Some aspects of human culture are universal, some are national, and others are particular to social classes or small groups. Culture is never static, and different cultures interact in different ways." Joseph S. Nye Jr. *The Future of Power,* 84.
[11] Emphasis mine. See Joseph S. Nye Jr. *The Future of Power,* 84.
[12] Ibid., 97.
[13] Puritan leader John Winthrop's seventeenth-century vision of the Massachusetts Bay Colony as a 'city upon a hill,' whose example the world would follow by choice rather than coercion, foreshadowed how the idiom of American exceptionalism might authorize alternative forms of international influence.
[14] Joseph S. Nye Jr. *The Future of Power*, 100.

political and social schisms carry the potential for the US to misapply hard power advantages or appear less attractive to partner nations, thus decreasing US power. Weaponized Narrative used against the US decreases the capacity for America to transform power resources into influence.

### The Ambiguous Nature of Weaponized Narrative in International Law

Even if a process existed to effortlessly attribute Weaponized Narrative strategies to its creator, what legitimate response options does a state have in the international system? Weaponized Narrative strategies are ambiguous in international law and behavioral norms and cannot be unambiguously scrutinized using traditional explanations of international *sovereignty, self-determination*, or *human rights*. For sovereignty, international law is definitive. States are entitled to territorial integrity, and violations of boundaries by acts of violence justify self-defense or declarations of war. In contrast, Weaponized Narrative does not violate territorial boundaries in a transparent fashion. Weaponized Narrative can influence human choices within state boundaries, but the international system lacks clearly defined cognitive boundaries.

*Sovereignty* is the right for a state to control its territorial boundaries. *Sovereign will* describes the connection between the state and its people. These two terms—sovereignty and sovereign will—are often mistakenly used as if they are interchangeable. In one example, Michael McFaul, U.S. ambassador to Russia from 2012 to 2014, stated his beliefs regarding Russian meddling in the 2016 US election: "Russia violated our sovereignty, meddling in one of our most sacred acts as a democracy—electing our president."[15] McFaul used the word sovereignty, but his accusation better resembled the concept of sovereign will. In the reality of international law, the closest thing to sovereign will is the concept of self-determination, which is the right of all peoples to determine for themselves their political, economic, and cultural destiny.[16]

[15] Greg Miller, Ellen Nakashima, and Adam Entous. "Obama's Secret Struggle to Retaliate against Putin's Election Interference - Washington Post." The Washington Post, June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.003a3de229b0.

[16] Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95 (June 2017): 21.

Weaponized Narrative is ambiguous because it can influence the choices of state populations but ultimately does not remove the right for the people to determine their destiny. Self-determination constructs or bolsters a state's connection with its people, but cognitive boundaries are not established or protected under international law unlike sovereignty, which is the right to control territorial boundaries. Sovereign cognitive boundaries protecting national identities and values are left to question. The idea of self-determination may conceptually parallel sovereignty but does not fit Russian Weaponized Narrative activity within the US. Any attempt by the US to delineate sovereign cognitive boundaries would be hindered by historical cases of American interference in other state self-determination pleas—Vietnam's struggle for independence would be an example. Self-determination is an international norm and sovereignty is international law, and Weaponized Narrative sidesteps norms and law unscathed.

*Human rights* violations are currently the closest arguments for Weaponized Narrative breaking international law. The intent of human right law under the International Covenant on Civil and Political Rights (ICCPR) is to protect the individual from the ruling government. As an example, Article 17 of the ICCPR states, "that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[17] For Russia's interference in the 2016 elections, it may seem that its influence activities in the US violated "the human rights of the owners of the various e-mail accounts, including John Podesta and several DNC officials," but in practice, Article 17 is restrained to applications like highlighting mass surveillance by governments observing their own citizens.[18] Russian Weaponized Narrative in the US brought indictments against Russian individuals and companies but remained ambiguous under international law in terms of its application for the Russian state.

US domestic law is the first rule-based line of defense against Weaponized Narrative. Two examples are the Federal Election Campaign Act (FECA) and the Foreign Agent Registration Act (FARA). The US Federal Election Commission agency administers FECA which prohibits "foreign nationals from making any contributions,

[17] Jens David Ohlin, "Did Russian Cyber Interference Violate International Law?" 1593.
[18] Ibid., 1593.

expenditures, independent expenditures, or disbursements for electioneering communications."[19] FARA, administered by the US Department of Justice, "establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law."[20]

Both FECA and FARA hold individuals and entities accountable to law but fail to address Russian state endorsement of Weaponized Narrative activities. Using the term, Weaponized Narrative, the US can begin to communicate behavioral norms expected of other nations. By tethering new laws and coercion methods to the media, methods, and intent of Weaponized Narrative the US can aid the effort to build sovereign cognitive boundaries.

## The Challenge for Democracy

Weaponized Narrative generates specific problems when employed against democracies. The most significant challenge is the direct clash with the values of democracy—liberty, truth, and freedom. Weaponized Narrative takes advantage of democracies' free speech and open information environments. The ambiguity of Weaponized Narrative generates "a lag time before the targeted democracies realize there is a problem."[21] Additionally, democracies are challenged when attempting to repel Weaponized Narrative by standard methods, such as deterrence by denial or deterrence by punishment. Democracies choosing to use Weaponized Narrative strategies in retaliation—fighting fire with fire—would result in misalignment between the actions and the values of a democratic state; in turn, this would lead to a decline of soft power and legitimacy.[22]

Sharp power and Weaponized Narrative strategies are at the leading edge of the new malicious style of great power competition between autocratic and democratic

[19] Robert Mueller, "Internet Research Agency Indictment." Department of Justice, February 16, 2018, 11. https://www.justice.gov/file/1035477/download.
[20] Ibid., 11.
[21] Juan Pablo Cardenal, *Sharp Power: Rising Authoritarian Influence*, 13.
[22] This statement may become less appropriate as conflict progresses from Gray Zone competition to total war.

states.[23] A report released by the National Endowment for Democracy (NED) commented that repressive regimes are not necessarily seeking to “win hearts and minds” with soft power efforts, but are instead seeking to influence targeted audiences by “manipulating or poisoning the information that reaches them” with sharp power.[24] Through Weaponized Narrative, “the generally unattractive values of authoritarian systems—which encourage a monopoly on power, top-down control, censorship, and coerced or purchased loyalty—are projected outward,” and presented as viable value systems when juxtaposed with exacerbated schisms within democracies.[25] Democracies are left struggling to find ways to uphold free and liberal information environments while defending against sinister attempts to subvert institutions, identity, and sovereign will.

### Freedom of Speech

A cornerstone of a free and liberal information environment is freedom of speech. Freedom of speech, however, is the core dilemma to resolve while protecting democracies from Weaponized Narrative strategies. Law, advancing communication technology, and censorship are present challenges for democracies defending against Weaponized Narrative. The US legal framework shields privacy and restricts domestic surveillance. Progressive global communication networks and intelligence gathering methods blur the requirements of privacy, surveillance, free speech, and defense. Such blurring is exacerbated by a legal framework written for a different era, one that did not “account for the inter-mingling of domestic and foreign communication—which is characteristic of social media—and information collected on or about another country’s populace may also include information from U.S. persons.”[26] The US legal framework cannot appropriately protect the political and social schisms from foreign influence if American surveillance infringes on privacy or censors freedom of speech.

[23] Ibid., 13.
[24] Ibid., 13.
[25] Ibid., 13.
[26] William Marcellino, Meagan L. Smith, Christopher Paul, and Lauren Skrabala. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1742.html.

In democratic free information environments, censorship ought to be impossible, equating to a golden age of free speech.[27] The US must remember, however, that freedom of speech is a *means* to uphold democracy, not an *end*.[28] Free speech in a democracy is meant to inform healthy debates, create a knowledgeable public, and hold powerful people and institutions accountable.[29] Conversely, foreign entities purposefully take advantage of free speech, manipulating this unguarded vulnerability that lacks alarms for distinguishing truth from falsehood, and attributing sources of information.[30] Within the territorial and cognitive borders of democratic states, freedom of speech brings together without prejudice those who support democracy, terrorism, and those interested in subverting democracy.

## Deterrence Challenges for Democracy

Deterrence is a coercive strategy which uses conditional threats to manipulate the behaviors of others.[31] The conditional threats used by democracies in response to Weaponized Narrative primarily align with a norms-based approach which "requires reinforcing certain values to the point where it is well understood that they must not be violated."[32]

Weaponized Narrative challenges the ability of democracies to deter by denial and/or punishment. Deterrence by denial is a conditional threat meant to "control the situation sufficiently in order to deny the opponent strategic options."[33] The democratic

[27] The golden age of speech is the capacity to spread ideas and reach an audience, no longer limited by access to expensive, centralized broadcasting infrastructure. Instead, the limit is the ability to garner and distribute attention. Currently, the flow of the world's attention is structured by just a few digital platforms: Facebook, Google, and Twitter. These companies—which hold themselves up as monuments of free expression—at their core are ad brokers to virtually anyone who wants to pay for the capacity to precisely target our eyeballs. See Zeynep Tufekci, "It's the (Democracy-Poisoning) Golden Age of Free Speech." WIRED, January 16, 2018. https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/.

[28] In an article entitled, "It's the (Democracy-Poisoning) Golden Age of Free Speech," Zeynep Tufekci, wrote that "what we are seeing now is that when free speech is treated as an end and not a means, it is all too possible to thwart and distort everything it is supposed to deliver."[28]

[29] Ibid.

[30] Ibid.

[31] Lawrence Freedman, *Deterrence*. Cambridge, UK; Malden, MA: Polity Press, 2004, 6.

[32] Ibid., 4.

[33] Ibid., 36.

cost of executing this option is a loss of legitimacy and authority due to reneging on proclaimed values. Denial requires the unwelcomed addition of controlling and surveilling free information environments, thereby encroaching on the liberties of privacy and freedom of speech.

In contrast, deterrence through punishment is a conditional threat that gives "powerful incentives to choose in a particular way."[34] In this option, the cost incurred by democracy is setting the conditions where an opponent recognizes the forecasted pain of directed incentives. Punishment options for democracies are limited. Weaponized Narrative used in revenge counters the values of democracy. Sanctions may not meet the threshold to deter an aggressor, and blowback from sanctions may affect the originator's economy. Military force could be an option but likely fails to reasonably met standards of legitimacy by law or international behavioral norms.

The US response to deter further Russian Weaponized Narrative aggression was a scaled down version of an initially stern plan. The initial plans called for the use of severe coercive instruments to include economic sanctions, damaging cyberattacks, and information warfare. The Washington Post reported from an undisclosed source that economic sanctions "would hit entire sectors of Russia's economy. One preliminary suggestion called for targeting technology companies including Kaspersky Lab, the Moscow-based cybersecurity firm."[35] Cyberattacks were to be combined with economic sanctions to disable Russian networks temporarily. Additionally, the US considered releasing embarrassing sensitive information concerning Putin and imposing personal sanctions against him.

In actual execution, the US began with diplomatic warnings before the US election followed by three post-election reactions. First, the US imposed economic sanctions targeted against Russian intelligence organizations with little economic footprint in the US.[36] Second, thirty-five Russian diplomats were ordered to leave the US, and the Russian-owned facilities were closed on Maryland's Eastern Shore and on

[34] Ibid., 36.
[35] Greg Miller, Ellen Nakashima, and Adam Entous, *Obama's secret struggle.*
[36] Ibid.

Long Island which were believed to have been used for intelligence purposes.[37] Third, digital bombs allegedly were implanted in the Russian network that could be triggered in a retaliatory cyberattack against future Russian aggression.[38]

The difficulty for American policymakers was in deciding what retaliatory action or form of coercion to pursue against Russia since a clear void existed in international laws and behavioral norms by which to justify those actions. The nature of Russia's Weaponized Narrative attack left the US with an evident commonsense awareness that its self-determination and sovereign will were violated. No formal international laws were broken. Without an immediate, evident, existential threat, the US had little justification for the use of severe coercive action against Russia.

## Conclusion

Weaponized Narrative wields power in the form of sharp power, which penetrates the information environment of an adversary and degrades national power by attacking culture, political values, and foreign policy. In international law and norms, Weaponized Narrative evades the rules of state sovereignty, self-determination, or human rights. The elusiveness of Weaponized Narrative clashes with liberal values creating unique challenges for democracies attempting to balance free speech, open information environments, privacy, surveillance, and security against unwanted foreign influence. When democracies elect to deter Weaponized Narrative via denial or punishment strategies, this carries a number of potential costs, from a loss in international legitimacy and prestige—due to reneging on values—to economic sanction blowback.

[37] Ibid.
[38] Ibid.

# Chapter 7

## Implications

> *In today's information age, we must recognize that the essential 'key terrain' is the will of a host nation's population...[This] permits us to gain the trust of skeptical populations, thus frustrating the enemy's efforts and suffocating their ideology.*
>
> General James N. Mattis, USMC, 2008

Wars can be fought militarily—with primary objectives including seizing ground, destroying enemy assets, and providing foreign aid. However, the military instrument of power is not always the primary means for achieving political outcomes. The cognitive battleground, involving a fight of narratives to direct the identity and *will* of the general public, has emerged as the new high-ground for inter-state competition. General Mattis' quote above, while originally in reference to irregular warfare, is ever relevant in today's contemporary conflicts with other states. Cognitive ground—the identity and *will* of the general public—has reemerged as the new high ground for inter-state competition. The US should heed the same warning, being mindful of protecting the American population against cognitive threats. As the US continues to reevaluate the relevance of the cognitive domain in war and conflict, then it must also consider how to harness cognitive capabilities and strategy development.

The objective of this thesis was to address two critical questions: 1) What key qualities distinguish the term Weaponized Narrative? and 2) How do these qualities explain recent Russian cognitive influence activity in the US? This thesis accomplished this by adding contextual understanding to the definition of Weaponized Narrative before comparing with other cognitive domain terms to extract distinct qualities. Next, this study demonstrated how Russian influence operations before, during, and after the 2016 US presidential election exhibited the intent, method, and media defined by Weaponized Narrative. Furthermore, this paper argued that the changing character of warfare, conflict, and competition in the information age is increasingly reliant on Clausewitzian Projects, sharp power, and strategies like Weaponized Narrative. Ultimately it proved that the term Weaponized Narrative conceptually adds value to the lexicon used to recognize, communicate, and formulate strategy in opposition to intricate cognitive threats.

Chapter 2 began by defining Weaponized Narrative as the use of story-based communications to foment political and social schisms with the intent to subvert an adversary's institutions, identity and/or will.  Weaponized Narrative manifest as a strategy and a *Clausewitzian Project* in the expanding cognitive battleground generated by blind human faith placed in advancing communication technologies.  Chapter 3 juxtaposed Weaponized Narrative with other cognitive domain terms to establish that the Weaponized Narrative term uniquely conveys the method of exacerbating social and political fissures in a long-term strategy.  The distinct analytical additions provided by the term Weaponized Narrative contribute to bridging societal lexical divides and enriching US ability to categorically identify, precisely communicate, and enhance the formulation of strategy against the threat of cognitive influence.

The case studies in Chapters 4 and 5 demonstrated that belligerent states like Russia had leveraged Weaponized Narrative as a sharp power meant to inject doubt, mistrust, and division into the liberal foundation of US identity.  Chapter 6 correlated the Weaponized Narrative term with state power.  In international relations, the relevance of Weaponized Narrative manifests as a sharp power and acts as a counterforce to soft power, and both share the target of broad public opinion and cultural attitudes. Advancements in technology have enabled a highly networked global society where liberal open information environments are particularly susceptible to Weaponized Narrative aggression.

## An Approach to Solution

No easy solutions exist for thwarting Weaponized Narrative aggression, but for democracy to thrive it must protect and secure the confidence and trust of the voter.  The general population is the most significant resource of democracy and the premier battleground for adversaries who wish to diminish liberal foundations.  The Weaponized Narrative term is one addition to a lexicon that needs expansion commensurate with the rise of sharp power.

In his book, *Pure Strategy*, Everett Dolman offers four fundamental principles to consider in designing a strategy with a complex adaptive system structure.[1] The four principles are *maximize nodes*, *maximize connections*, *maximize response sets*, and *minimize top-down control*. These principles apply to the strategies developed in opposition to Weaponized Narrative because of the complexity of coordination across laws, norms, and institutional or individual interests.

The principle of *maximizing nodes* is the recognition that the target of Weaponized Narrative is primarily the general public. However, the mass population is also the front line of defense in liberal open information environments. Harvesting the general public in collective defense maximizes nodes and will be vital to the success of future strategies against cognitive threats. The *maximizing connections* principle centers on transparency and the need to adequately inform institutions and the general public that they are under cognitive attacks. Weaponized Narrative is a useful term to propagate in a cognitive threat level scale.

*Maximizing response sets* is a principle concerning education. President Dwight Eisenhower said, “Information and education are powerful forces in support of peace. Just as war begins in the minds of men, so does peace.”[2] Incorporating the general population in defense strategies requires increasing their awareness and knowledge of cognitive threats. Countries such as Estonia and Italy are incorporating digital-literacy courses in grade schools to identify and communicate threats like Weaponized Narrative. The US should consider digital literacy, for example, as a standard in public education as is the case in Estonia and Denmark.

Finally, the principle of *minimizing top-down control* is maximizing empowerment by collaboration and reporting. Increased collaboration between government and commercial information-based businesses will help to establish effective measures and norms to weed out disinformation, falsehood, and propaganda. Institutions and individuals will feel empowered by education and a provided avenue to report suspected Weaponized Narrative activity, much like observed crime is reported to police,

[1] Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*. Cass Series--Strategy and History 6. London; New York: Frank Cass, 2005, 179.
[2] William M. Chodkowski, “The United States Information Agency.” *American Security Project*, November 2012, 9.

and fires are reported to the fire department. Feedback is the linchpin to reporting and closes the loop to reinforce empowerment. The response or lack of response to reporting will determine the trust and confidence in a system that tracks and produces evidence to denounce the effects of Weaponized Narrative.

### A Cognitive Organization and Cognitive Soldier

The 2018 US NSS and NDS acknowledge that adversaries are seeking advantages by weaponizing information and that US efforts to counter exploited information is tepid, fragmented, and lacks sustained focus.[3] The NSS attributes this problem to a lack of adequately trained professionals.

The US lacks an entity—and assigned personnel—responsible for optimizing the six subcomponents of informational power; military information, public diplomacy, public affairs, communication resources, international forums, and venues for announcements. Is it time to create an organization for cognitive soldiers to lead the optimization and integration of the national information instrument of power? A cognitive organization and the respective personnel would house unique responsibilities and skillsets to sift through the white noise generated by increasing volumes and velocity of information. Said differently, the cognitive soldier would be responsible for leading the US in neocortical warfare.

Neocortical warfare—to control the behavior of enemies without destruction—has four characteristics. First, competition, conflict, and resolutions are permanents features in human existence. Second, neocortical warfare is continuous and constant. Third, "using the adversary's lexicon, syntax and representational systems allows the neocortical warrior to lead the adversary through the cycle of observation, orientation, decision and action."[4] Fourth, a coercive physical force of arms must be preserved or created to support the neocortical warrior by introducing "shock, surprise and terror in the adversary's external world…to fuel the nightmares and disorientation sought in the enemy's internal world."[5]

[3] "National Security Strategy of the United States of America." US Government, December 2017.
[4] Richard Szafranski, "Neocortical Warfare? The Acme of Skill," in *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997), 395–416, 408.
[5] Ibid., 408.

The information environment involves all national instruments of power—diplomatic, informational, military, and economic—resulting in many organizations that have piecemeal functions in national informational power. Budgets drive the language and perspectives of bureaucracies that contribute to the informational instrument of power.[6] One budgetary disadvantage is bureaucracies may view information problems by the available budgeted tools instead of the most effective cognitive approach to influence and protect human will.[7] One example is shown in US cybersecurity: "Within various regulatory agencies-for example, the Securities and Exchange Commission, Federal Energy Regulatory Commission, Federal Communications Commission, and Federal Deposit Insurance Corporation-see it as a regulatory problem; they are inserting cybersecurity into their regimes but as consistent with their allowed toolkits."[8] Similar to cybersecurity, if the components of informational power reside in different organizations, who is responsible for the defense against sharp power and Weaponized Narrative, or to develop cognitive influence expertise for the long-term strategic narrative of the US?

The purpose and responsibility of a cognitive organization and soldiers is to integrate and optimize information across all instruments of power for the protection and influence of human-will in support of national security (see Figure 6, below). The cognitive soldier concept could house a delicate mix of government and private business personnel, who wield a unique authority that is physically borderless but cognitively bound by US liberal values and ethical standards.[9]

[6] Martin Libicki, *Cyberspace in Peace and War (Transforming War)*. Naval Institute Press, 2016, 70.

[7] Ibid., 70.

[8] Ibid., 70.

[9] In the article “Neocortical Warfare? The Acme of Skill,” Richard Szafranski asked for the same civilian and government mix: “neocortical warfare requires a better integrated, joint civilian and military national security control force with both armed and unarmed elements. It must be capable of sustained, cooperative, and non-lethal presence in every area we have interests.

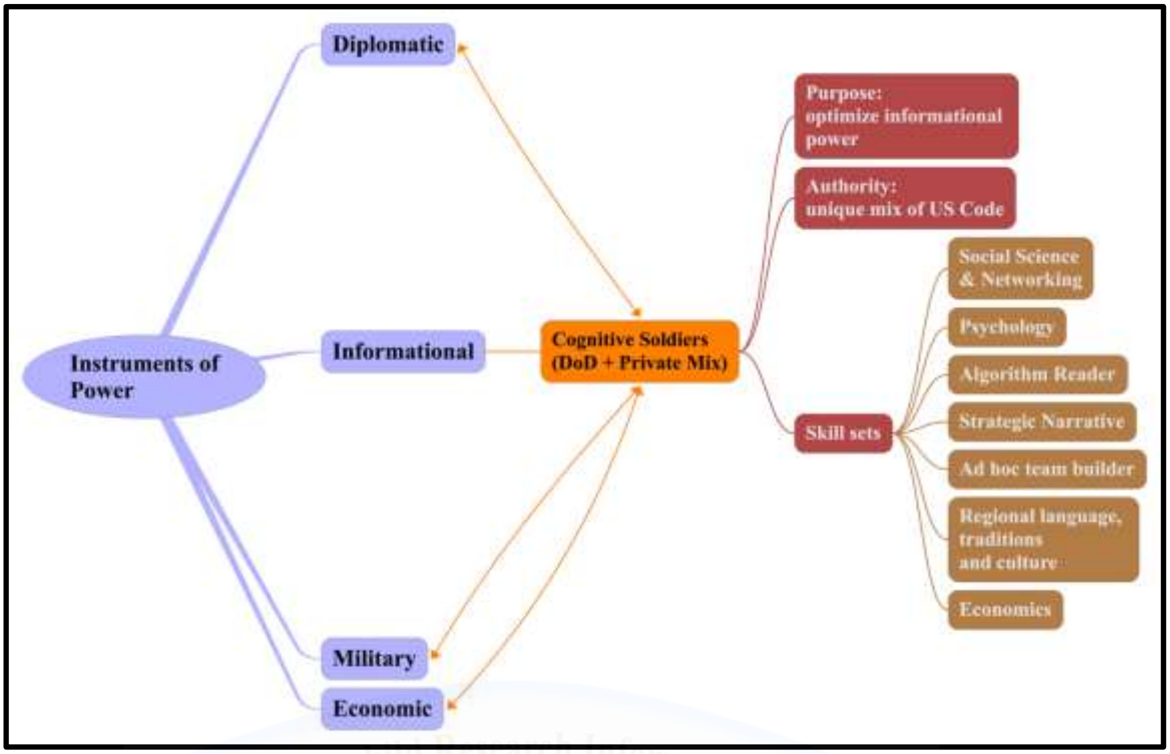

Diplomatic
Purpose: optimize informational power
Authority: unique mix of US Code
Social Science & Networking
Psychology
Algorithm Reader
Instruments of Power
Informational
Cognitive Soldiers (DoD + Private Mix)
Skill sets
Strategic Narrative
Ad hoc team builder
Regional language, traditions and culture
Economics
Military
Economic

**Figure 6: Cognitive Soldier**
Source: Author's Original Work

The cognitive soldier concept is neither new nor revolutionary. In 1953, the United States Information Agency (USIA) was created under the administration of President Eisenhower as an "independent executive agency responsible for American public diplomacy."[10] The mission of USIA was to "understand, inform and influence foreign publics in promotion of the national interest, and to broaden the dialogue between Americans and U.S. institutions, and their counterparts abroad."[11] The USIA was disbanded in 1999 due to severe budget and personnel cuts as the perceived threat from the Soviet Union evaporated. After disbanded, USIA was functionally integrated with the Public Diplomacy and Public Affairs Office in the US Department of State. Reviving

[10] William M. Chodkowski, "The United States Information Agency," 9.

[11] The four functions of USIA were: (1) to advocate US policies in meaningful ways to foreign cultures, (2) provide information about the people, values, and institutions that influence US policy, (3) help American citizens and institutions build strong long-term relationships with their counterparts overseas, and (4) advise on the ways in which foreign attitudes will have direct bearing on the effectiveness of US policies. Chodkowski, William M. "The United States Information Agency," 9.

and tweaking the authorities and resources of USIA could resemble future options to fulfill a cognitive soldier organization.

How would the US value cognitive soldiers vowed to protect a US-led liberal democratic order? William McNeill discusses in his book, *The Pursuit of Power*, how the definition of a soldier came into question as artillerymen first emerged on the battlefield and seemed to subvert accepted social norms of heroism and worthiness: "A weapon that could be used to kill soldiers impersonally and at a distance of more than half a mile offended deep-seated notions of how a fighting man ought to behave. Risk ceased to be symmetrical in such a situation, and that seemed unjust. The skill of an obscure, mathematical, and technological kind threatened to make old-fashioned courage and muscular prowess useless."[12] Artillerymen were seen as unjust, lacking muscular prowess and heroic characteristics, and were undervalued until social norms changed. Technology progressed warfare through the crossbow, rifle, artillery, airplane, ballistic missile, cyber, and now a heavy reliance on algorithms and machine learning. Each technological progression in many ways takes humanity a step further from muscular heroism rooted in traditional hand-to-hand combat.

Clausewitz reminds us that however far removed combat takes place from a physical encounter, "combat is the only effective force in war; its aim is to destroy the enemy's forces as a means to a further end. The combat mentality holds true even if no actual fighting occurs, because the outcome rests on the assumption that if it came to fighting, the enemy would be destroyed."[13] Physical or economic force is the predominant understanding of how war is conducted. The US should acknowledge the rise of cognitive ground relevance in the changing character of war and conflict in the information age. The information domain is a place for humans to exert cognitive force and conduct cognitive combat in war, conflict, and competition. The social norms of acceptance and valuating the works a cognitive soldier must catch up and address the cognitive capability gaps of the US. America should foster an environment for the cognitive soldier concept to emerge and be valued as worthy heroes in the collective

[12] William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*. University of Chicago Press (1984), Edition, 1984, 172.

[13] Carl von Clausewitz, Michael Eliot Howard, and Peter Paret, *On War*. First paperback printing (Princeton, NJ: Princeton University Press, 1989), 97.

defense of democracy. In future war or conflict, the physical domain will at times become subordinate to the cognitive domain.

Russia and others around the globe will continue to use cognitive attacks against democracies. Some influence operations will seek immediate political goals, and others have a "broader, long-term aim: weakening Western democracies by undermining trust in institutions and dividing their citizens against each other."[14] Rand Waltzman, part of the RAND Corporation and former manager at the US Defense Advanced Research Projects Agency (DARPA), explains that "when target forces start to counter these [Russian] efforts and/or expose them on a large scale, the Russians are likely to accelerate the improvement of their techniques…in other words, an information-warfare arms race is likely to ensue."[15]

Russia and China created new organizations for information warfare in the wake of advancing network communication technology, sharp power, and Weaponized Narrative. Both countries are also moving towards independent internets. China specifically views internet censorship as a question of sovereignty and encourages other nations to do the same.[16] Other nations are taking actionable steps towards organizing and adapting to the changing character of conflict and competition in the information age.

## Conclusion

The use of the Weaponized Narrative term provides a framework of elements to understand cognitive threats in the information age. The elements—intent (to subvert), method (to foment schisms), and medium (story-based communication)—can traverse societal sectors and security classification levels and retain the same meaning. The elements of the Weaponized Narrative term strengthen the available lexicon to enhance the collaborative development of strategies against cognitive threats. Propagated use and understanding of this term will aid identification of cognitive threats and improve effective communication. Weaponized Narrative—a cognitive conceptual tool—can enhance the NDS dictate to cultivate workforce talent for a lethal agile force requiring the

[14] Briefing: Russian Disinformation, "The Discord Amplifier," *The Economist*, Feb 24, 2018.
[15] Special Report, "Waging War with Disinformation," *The Economist*, January 25, 2018.
[16] Wataru Kodaka, "China Toughens Web Censorship, Encourages Others to Follow." Nikkei Asian Review, December 5, 2017. https://asia.nikkei.com/Politics-Economy/Policy-Politics/China-toughens-web-censorship-encourages-others-to-follow.

ability to integrate new capabilities, adapt warfighting approaches, and change business practices to achieve mission success in both physical battle and cognitive warfare.[17]

[17] "Summary of the 2018 National Defense Strategy of The United States of America." Accessed February 1, 2018. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

## Appendix A

### Expanded Descriptions of Cognitive Domain Terms

**Weaponized Narrative:** the use of story-based communication to foment political and social schisms with the intent of subverting an adversaries' institutions, identities, and/or will.

**Propaganda / Computational Propaganda:** Richard Nelson in his 1996 work *A Chronology and Glossary of Propaganda in the United States* defines propaganda as: “a systematic form of purposeful persuasion that attempts to influence the emotions, attitudes, opinions, and actions of target audiences for ideological or political purposes through the transmission of one-sided messages (which may or may not be factual) via mass and direct media channels.”[1] The military Joint Publication 3-13.2 defines propaganda as “any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.”[2] Computational propaganda “is a new term for the use of social media, big data, autonomous agents, and related technologies for political manipulation. This can range from relatively benign amplification of political messages to insidious state-sponsored trolling and disinformation.”[3]

**Command of the Trend (Weaponized Social Media):** “The trend list is a quick way to review the most discussed topics at a given time. And according to a 2011 Cornell University study on social media, a trending topic “will capture the attention of a large audience for a short period.” The trend list thus “contributes to agenda setting mechanisms.” Utilizing existing online networks in conjunction with automatic “bot” accounts, foreign agents can insert propaganda into a social media platform, create a trend, and rapidly disseminate the message faster and cheaper than through any other medium in history. Such efforts represent a relatively novel and increasingly dangerous means of weaponizing social media.”[4]

Command of the Trend hinges on 4 factors: “(1) A message that fits an existing, even if obscure, narrative (2) A group of "true believers” predisposed to the message (3) A relatively small team of agents or cyber warriors (4) A network of automated "bot"

[1] Richard Nelson. *A Chronology and Glossary of Propaganda in the United States*. Westport, CT: Greenwood Press, 1996.

[2] Joint Publication 3-13.2: *Psychological Operations*, 2010.

[3] Matt Chessen. *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy...and What Can Be Done About It*.” September 29, 2017. https://weaponizednarrative.asu.edu/publications.

[4] Jarred Prier. “The Command of the Trend: Social Media as a Weapon in the Information Age.” SAASS Air University, 2017. http://www.dtic.mil/docs/citations/AD1039253.

accounts. There are three methods for controlling what is trending on social media: trend distribution, trend hijacking, and trend creation."[5]

**Disinformation / Misinformation:** Disinformation is deliberately deceptive information, and misinformation is inaccurate information.[6] Misinforming and disinforming are types of information behavior as the features below describe.[7]

**Table 5: Distinctions Between Information, Misinformation, and Disinformation**

| | **Information** | **Misinformation** | **Disinformation** |
|---|---|---|---|
| **True** | Y | Y/N | Y/N |
| **Complete** | Y/N | Y/N | Y/N |
| **Current** | Y | Y/N | Y/N |
| **Informative** | Y | Y | Y |
| **Deceptive** | N | N | Y |
| Y = Yes; N = No; Y/N = Could be Yes and No, depending on context & time | | | |

Source: 'Plz RT': *A Social Diffusion Model of Misinformation and Disinformation for Understanding Human Information Behaviour,* Karlova.

**Cognitive Hacking:** "Gaining access to or breaking into a computer information system to modify certain user behaviors in a way that violates the integrity of the entire user information system. Cognitive hacking can be either covert, which includes the subtle manipulation of perceptions and the blatant use of misleading information, or overt, which includes defacing or spoofing legitimate forms of communication to influence the user. Cognitive hacking differs from social engineering, which, in the computer domain, involves a hacker's psychological tricking of legitimate computer system users to gain information, e.g., passwords, in order to launch an autonomous attack on the system."[8]

**Military Information Support Operations (MISO):** "Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."[9]

[5] Ibid.

[6] Natascha A. Karlova, and Karen E. Fisher, "'Plz RT': A Social Diffusion Model of Misinformation and Disinformation for Understanding Human Information Behaviour," 2012.

[7] Ibid.

[8] George Cybenko, Annarita Giani, and Paul Thompson. "Cognitive hacking: A battle for the mind." Computer 35, no. 8 (2002): 50-56.

[9] *DOD Dictionary of Military and Associated Terms*, 2018. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

**Information Operations (IO):** The DoD Dictionary of Military and Associated Terms defines IO as "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."[10] The Marine Corp Warfighting Publication 3-40.4 further describes IO as a complement and facilitator in the "traditional use of military force but in some instances may stand alone as a deterrent option. …Capabilities relevant to IO include, but are not limited to, psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), physical attack, information assurance (IA), computer network operations (CNO), public affairs (PA), and civil-military operations (CMO).[11]

**Psychological Operations (PSYOP):** "Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."[12]

MCWP 3-40.4 states "PSYOP shape attitudes and influence behavior…At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements or communiques. At the operational level, PSYOP can include the distribution of leaflets, radio and television broadcasts, and other means of transmitting information that provides information intended to influence a selected group. It may be used to encourage enemy forces to defect, desert, flee, surrender, or take any other action beneficial to friendly forces. At the tactical level, PSYOP include face-to-face contact and the use of loudspeakers or other means to deliver PSYOP messages."[13]

**Military Deception:** "Military deception operations are actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[14]

**Public Affairs (PA): "**Communication activities with external and internal audiences. See also *command information*; *public information*."[15]

- **Command information** — "Communication by a military organization directed to the internal audience that creates an awareness of the organization's goals, informs them of significant developments affecting them and the organization, increases their effectiveness as ambassadors of the organization, and keeps them informed about what is going on in the organization."[16]

[10] Ibid.

[11] MCWP, *MCWP 3-40.4: Marine Air-Ground Task Force Information Operations*. US Marine Corps, n.d.

[12] *Joint Publication 3-13.2: Psychological Operations,* 2010.

[13] MCWP, *MCWP 3-40.4: Marine Air-Ground Task Force Information Operations*.

[14] *DOD Dictionary of Military and Associated Terms,* 2018.

[15] Ibid.

[16] *DOD Dictionary of Military and Associated Terms,* 2018.

- **Public information —** "Within public affairs, information of a military nature, the dissemination of which is consistent with security and approved for public release."[17]
- **Public affairs assessment —** "An analysis of the news media and public environments to evaluate the degree of understanding about strategic and operational objectives and military activities and to identify levels of public support."[18]

**Theme / Message:** Webster Dictionary defines theme as "a subject or topic of discourse or of artistic representation."[19] Joint Publication 6-0 defines message as "any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication."[20] In other words, "a narrowly focused communication directed at a specific audience to support a specific theme."[21]

[17] Ibid.

[18] Ibid.

[19] "Theme," Merriam-Webster.com. Accessed February 26, 2018. https://www.merriam-webster.com/dictionary/theme.

[20] *DOD Dictionary of Military and Associated Terms*, 2018.

[21] Ibid.

# Appendix B

## Weaponized Narrative: China and ISIS

China is also using Weaponized Narrative to achieve geopolitical objectives in the South China Seas (SCS). China enabled a strong D-I-M-E foothold in the SCS by blending a unified *Asianism* narrative while simultaneously undermining US led democratic order. Although Weaponized Narrative had not been coined, twenty years ago the US was describing the characteristics, "the world is being swept by powerful revivals of religions, and new assertions of ethnic identities, paradoxically backed by certain nation-states. China is emerging as the driving force of an ethnic 'Asianism.'"[1]

China also recognized the utility of cyberspace in Weaponized Narrative employment and defense. The US views the internet as a tool for democracy and a liberal global economy based on free-trade. A position opposite of China's cyber sovereignty narrative, which "accentuates the instability and greater dissent that can accrue with a border-spanning open internet."[2] Chinese President Xi Jinping said, "the spread of information on the internet poses an unprecedented challenge to the sovereignty and security of countries."[3] China's combined use of the Asianism narrative and Weaponized Narrative is described by Sun Tzu's statement; "attacking with the assurance of taking the objective is a matter of attacking a place that the enemy is not defending. You can be sure that your defense will hold when you defend a place that the enemy will not attack. And so, facing an expert at attacking, an enemy will not know what to defend, and facing an expert at defending, an enemy will not know what to attack."[4] In the cognitive realm, China is setting defenses with an Asianism narrative deeply rooted in historic culture, which is challenging to target directly as a democratic nation.

Additionally, China is attacking Western democracy with Weaponized Narrative, which is challenging to defend based on open internet and free speech values found in Western democracies. The combination effectively brought US military advantage and power second to a well-established cognitive battlefield in the SCS. Moreover, the combination constrains US military power in the SCS by not exactly knowing where to attack or what to defend. China, for the moment, has seized the upper hand.

The rise of ISIS highlighted the impact Weaponized Narrative can have on identity. Weaponized Narrative and cyberspace combined to generate a low-cost highly effective means for guerrilla organizations to negate US military advantage and power. In an interview for a Fifth Domain article, Dr. Ajit Maan, president of Narrative Strategies and affiliate faculty with the Center for Narrative Conflict Resolution,

[1] Lawrence Freedman, *Makers of Modern Strategy*. Edited by Peter Paret. Princeton, NJ: Princeton University Press, 1986.

[2] Ibid.

[3] Wataru Kodaka, "China Toughens Web Censorship, Encourages Others to Follow." Nikkei Asian Review. Accessed March 27, 2018. https://asia.nikkei.com/Politics-Economy/Economy/China-toughens-web-censorship-encourages-others-to-follow.

[4] Sun Zi, "The Art of War," Translated by Gary J. Bjorge. Fort Leavenworth, KS: Department of Military History, US Army Command and General Staff College, 2005.

mentioned that “despite the West’s claims otherwise, ‘Islam is under attack’ resonates with ISIS followers in many forms. Narrative provides and determines the meaning of events…events don’t speak for themselves. Narratives speak for events.”[5] The Weaponized Narrative of ISIS and other violent extremist organizations (VEO) constrain US military power by confusing where and how military force should be applied.

For over 15 years the US has been in conflict with extremist Islamic groups based on the fundamental religious ideas of Sayyid Qutb. He presents an ideology that freedom for humankind can only be secured under the rule of Islamic leadership to ensure that humankind has an unhindered choice to follow God under Sharia Law.[6] Qutb’s ideas are anti-modernization, anti-globalization, anti-liberal democracy. However, Qutb’s ideology cannot be ignored and should be addressed in US political end-states.[7]

VEO Weaponized Narratives challenge the US as it struggles to find the best approach to defeat VEOs which are intertwined in Islam resulting in fractured wills and identities in the US. VEOs like ISIS directly challenged the identity of many US citizens by infusing the idea that Muslims should not attack Muslims, or that man-made constitutions should not take precedence over the commandments of Islam. This confusion results in cases like the Fort Hood mass shooting in 2009, where a US Muslim soldier killed and injured over 40 Americans.[8] Cases like this generate strong emotions to strengthen US resolve or give reason to doubt US governance. Rifts in identity are intensified in US culture to undermine democratic order. In recent years the US has seen Weaponized Narrative manifest in altered American identities willing to join and fight with ISIS. The effect constrains US military advantage and power by shifting threats to the “hearts and minds” of individuals; making the threat nearly formless and difficult to target.

[5] Brad D. Williams, “Narrative, Cyberspace and the 21st Century Art of War.” Fifth Domain, January 25, 2018. http://www.fifthdomain.com/home/2017/01/22/narrative-cyberspace-and-the-21st-century-art-of-war/.

[6] Sayyid Qutb, *Milestones*. Islamic Book Service, 2006.

[7] The ideology of Qutb presents a very symmetric conventional brute force clash against the ideology of liberal democracies. Disproving each idea of Qutb may not be necessary but a vision, narrative, and material political solution must be presented to express how mainstream Islam and liberal democracy can co-exist in a manner acceptable to the populous. US strategists will need this political answer to nest military objectives, operational approaches, and some tactical execution. Although some audiences could care less about the ideological clash–bandwagoning only for personal gain–the post-conflict environment will be plagued with the unchallenged ideology of Qutb. The result is a never-ending war of whack-a-mole, or short-lived peace until the next outburst rooting from Qutb’s ideology. This is particularly important because the US is an external actor in southwest Asia, and Qutb’s ideology can always retreat into nationalist motivations.

[8] Anita Belles Poerterfield and John Porterfield, “Death on Base, The Fort Hood Massacre.” Denton, TX: University of North Texas Press, 2015.

# Bibliography

Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake New in the 2016 Election." *The Journal of Economic Perspectives* 31, no. 2 (Spring 2017): 211–35.

Allenby, Braden. "The Age of Weaponized Narrative." *Issues in Science and Technology*, Summer 2017: 65-70.

———. White Paper on Weaponized Narrative. Weaponized Narrative Initiative, 2017. https://weaponizednarrative.asu.edu/publications/weaponized-narrative-white-paper-0.

Allenby, Braden, and Joel Garreau. "Weaponized Narrative Is the New Battlespace." Defense One, January 3, 2017. http://www.defenseone.com/ideas/2017/01/weaponized-narrative-new-battlespace/134284/.

———. *Weaponized Narrative: The New Battlespace*. Weaponized Narrative Initiative, 2017. https://weaponizednarrative.asu.edu/publications/weaponized-narrative-new-battlespace-0.

Astorino-Courtois, Allison, ed. "A Cognitive Capabilities Agenda: A Multi-Step Approach for Closing DoD's Cognitive Capability Gap." An SMA White Paper from the Strategic Multi-Layer Assessment Office, 2017.

Briefing: China and the West. "At the Sharp End." *The Economist*, December 16, 2017.

Briefing: Russian Disinformation. "The Discord Amplifier: The Divided West Is Particularly Vulnerable to Russian Disinformation Campaigns, Whether Old-Fashioned or High-Tech." *The Economist*, February 24, 2018.

Business: Social Media. "Facebook Unfriended: Russian Meddling Is Only One Challenge Facing the Social-Networking Giant." *The Economist*, February 24, 2018.

Cardenal, Juan Pablo, Jacek Kucharczyk, Grigorij Mesežnikov, Gabriela Pleschová, Christopher Walker, and Jessica Ludwig. Sharp Power: Rising Authoritarian Influence. National Endowment for Democracy, 2017.

Carr, E. H. *The Twenty Years' Crisis, 1919-1939*. London: Macmillan/Springer Nature, 2016.

Chen, Adrian. "The Agency." *The New York Times*, June 2, 2015, sec. Magazine. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

———. "The Real Paranoia-Inducing Purpose of Russian Hacks." *The New Yorker*, July 27, 2016. https://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks.

Chessen, Matt. “The MADCOM Future:  How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy...and What Can Be Done about It.,” September 29, 2017. https://weaponizednarrative.asu.edu/publications.

Chivvis, Christopher S. *Understanding Russian “Hybrid Warfare” And What Can Be Done About It*. RAND Corporation, Santa Monica, Calif., 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

Chodkowski, William M. “The United States Information Agency.” *American Security Project*, November 2012, 9.

Cialdini, Robert B. *Influence: The Psychology of Persuasion*. New York, NY: Collins Business, 2007.

Clausewitz, Carl von, *On War*. Michael Eliot Howard, and Peter Paret trans. and eds. First paperback printing. Princeton, NJ: Princeton University Press, 1989.

Coats, Daniel R. Statement for the Record:  Worldwide Threat Assessment of the US Intelligence Community, 2018.

“Cognitive | Definition of Cognitive by Merriam-Webster.” Accessed April 19, 2018. https://www.merriam-webster.com/dictionary/cognitive.

Cukier, Kenneth, and Viktor Mayer-Schoenberger. “The Rise of Big Data: How It’s Changing the Way We Think about the World.” *Foreign Affairs* 92 (2013): 28.

Cybenko, George, Annarita Giani, and Paul Thompson. “Cognitive Hacking: A Battle for the Mind.” *Computer 35*, 2002.

Dolman, Everett C. *Pure Strategy: Power and Principle in the Space and Information Age*. Cass Series--Strategy and History 6. London: Frank Cass, 2005.

Ellul, Jacques. *Propaganda:  The Formation of Men’s Attitudes*. New York, NY: Vintage Books, 1962.

Ewing, Philip. “Russians Targeted U.S. Racial Divisions Long Before 2016 And Black Lives Matter.” NPR.org. Accessed March 26, 2018. https://www.npr.org/2017/10/30/560042987/russians-targeted-u-s-racial-divisions-long-before-2016-and-black-lives-matter.

Feldscher, Kyle. “Mark Warner: It’s Time for the US to Create a Cyber Strategy to Fight Back against Russia, China.” Washington Examiner. Accessed November 29, 2017. http://www.washingtonexaminer.com/mark-warner-its-time-for-the-us-to-create-a-cyber-strategy-to-fight-back-against-russia-china/article/2639686.

Finn, Ed. *What Algorithms Want: Imagination in the Age of Computing*. Cambridge, MA: The MIT Press, 2017.

Freedman, Lawrence. *Deterrence*. Cambridge, UK; Malden, MA: Polity Press, 2004.

Frenkel, Sheera. “After Florida School Shooting, Russian ‘Bot’ Army Pounced.” *The New York Times*, sec. Technology. Accessed March 27, 2018. https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html.

Fuller, J. F. C. *Foundations of the Science of War.* Place of publication not identified: Books Express Publishing, 2012.

Galeotti, Mark. “The ‘Gerasimov Doctrine’ and Russian Non-Linear War.” *In Moscow’s Shadows* (blog), July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Garreau, Joel, and Braden Allenby. *WNI Podcast Episode #1: What Is Weaponized Narrative?*, n.d. https://itunes.apple.com/us/podcast/weaponized-narrative-initiative/id1238897299?mt=2.

Giles, Keir. *Handbook of Russian Information Warfare*. NDC Fellowship Monograph Series; 9. Rome, Italy: NATO Defence College Research Division, 2016. http://www.ndc.nato.int/download/downloads.php?icode=506.

Gilpin, Robert. *War and Change in World Politics*. Transferred to digital printing. Cambridge: Cambridge Univ. Press, 2002.

Glenn, Mike. “A Houston Protest, Organized by Russian Trolls.” Houston Chronicle, February 20, 2018. https://www.houstonchronicle.com/local/gray-matters/article/A-Houston-protest-organized-by-Russian-trolls-12625481.php.

Hall, Wayne Michael. *Stray Voltage:  War in the Information Age*. Annapolis, MD.: Naval Institute Press, 2003.

Herrman, John. “If Everything Can Be ‘Weaponized,’ What Should We Fear?” *The New York Times*, March 14, 2017, sec. Magazine. https://www.nytimes.com/2017/03/14/magazine/if-everything-can-be-weaponized-what-should-we-fear.html.

Herrmann, Jon. “Nine Links in the Chain:  The Weaponized Narrative, Sun Tzu, and the Essence of War.” The Strategy Bridge, July 27, 2017. https://weaponizednarrative.asu.edu/publications/nine-links-chain.

Ignatius, David. “Opinion | Russia’s Radical New Strategy for Information Warfare.” *Washington Post* (blog), January 18, 2017. https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.

Ikenberry, G. John. *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order*. Princeton Studies in International History and Politics. Princeton, NJ: Princeton Univ. Press, 2011.

“Influence Operations Ops, Propaganda, Deception, Counterpropaganda.” Accessed April 20, 2018. http://www.au.af.mil/info-ops/influence.htm#definitions.

“Instruments of National Power.” *The Lightning Press SMARTbooks* (blog), September 20, 2014. https://www.thelightningpress.com/the-instruments-of-national-power/.

Intelligence Community Assessment. “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution,” January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Isachenkov, Vladimir. “Russia Military Acknowledges New Branch: Info Warfare Troops | World News | US News.” Associated Press. Accessed November 29, 2017. https://www.usnews.com/news/world/articles/2017-02-22/planes-tanks-ships-russian-military-gets-massive-upgrade.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.

Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, 2010.

Joint Publication 3-13: Information Operations, 2012.

Joint Publication 3-13.2: Psychological Operations, 2010.

Kahneman, Daniel. *Thinking, Fast and Slow*. 1st ed. New York, NY: Farrar, Straus and Giroux, 2011.

Karlova, Natascha A., and Karen E. Fisher. “‘Plz RT’: A Social Diffusion Model of Misinformation and Disinformation for Understanding Human Information Behaviour,” Paper presented at the Proceedings of ISIC the information behaviour conference. Tokyo, Japan, 2012, 17.

Kim, Lucian. “What Was Russia’s Role In 2016 U.S. Election? 2 Former KGB Officials Weigh In.” NPR.org, November 11, 2017. https://www.npr.org/sections/parallels/2017/11/11/563287218/what-was-russias-role-in-2016-u-s-election-2-former-kgb-officials-weigh-in.

Kodaka, Wataru. “China Toughens Web Censorship, Encourages Others to Follow.” *Nikkei Asian Review*, December 5, 2017. https://asia.nikkei.com/Politics-Economy/Policy-Politics/China-toughens-web-censorship-encourages-others-to-follow.

Leaders. “The Meddler, Why the West’s Response Is Inadequate.” *The Economist*, February 24, 2018.

Libicki, Martin. *Cyberspace in Peace and War (Transforming War)*. Annapolis, MD: Naval Institute Press, 2016.

Liddell Hart, Basil Henry. *Strategy*. 2nd rev. ed. New York: Meridian, 1991.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. London: Frank Cass, 2004.

Lucas, Ryan. “How Russia Used Facebook To Organize 2 Sets of Protesters.” NPR.org. Accessed December 20, 2017. https://www.npr.org/2017/11/01/561427876/how-russia-used-facebook-to-organize-two-sets-of-protesters.

MacKenzie, Donald. *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (Inside Technology). The MIT Press (1993), Edition: Reprint, 478 pages, 1993.

Madrigal, Alexis. “15 Things We Learned from the Internet Giants.” Defense One. Accessed March 22, 2018. http://www.defenseone.com/politics/2017/11/15-things-we-learned-internet-giants/142279/.

Mahaffee, Dan. “We’ve Lost the Opening Info Battle against Russia; Let’s Not Lose the War.” Defense One. Accessed March 25, 2018. http://www.defenseone.com/ideas/2018/02/weve-lost-opening-info-battle-against-russia-lets-not-lose-war/146212/.

Marcellino, William, Meagan L. Smith, Christopher Paul, and Lauren Skrabala. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1742.html.

McNeill, William H. *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*. Chicago, IL: University of Chicago Press 1984.

MCWP. MCWP 3-40.4: Marine Air-Ground Task Force Information Operations. US Marine Corps, n.d.

Miller, Greg, Ellen Nakashima, and Adam Entous. “Obama’s Secret Struggle to Retaliate against Putin’s Election Interference.” *The Washington Post*, June 23, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.003a3de229b0.

Morgenthau, Hans J. "The Evil of Politics and the Ethics of Evil." Ethics 56, no. 1 (1945): 1-18. http://www.jstor.org/stable/2988705.

Mueller, Robert. "Internet Research Agency Indictment." Department of Justice, February 16, 2018. https://www.justice.gov/file/1035477/download.

National Security Strategy of the United States of America. US Government, 2017.

Nelson, Richard. *A Chronology and Glossary of Propaganda in the United States*. Westport, CT: Greenwood Press, 1996.

Nye Jr., Joseph S. *The Future of Power*. New York: Public Affairs, 2011.

Ohlin, Jens David. "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Cornell Law Faculty Publications* 95 (June 2017): 1579–98.

Olcott, Anthony. "Institutions and Information: The Challenge of the Six Vs." ISD Working Paper in New Diplomacy. Georgetown University: Institute for the Study of Diplomacy, 2010.

Ophardt, Jonathan A. "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield." *Duke Law & Technology Review*, no. 3 (2010): 27.

Paret, Peter, Gordon Alexander Craig, and Felix Gilbert, eds. *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*. Princeton Paperbacks. Princeton, NJ: Princeton University Press, 1986.

Parlapiano, Alicia. "The Propaganda Tools Used by Russians to Influence the 2016 Election." *The New York Times*, February 16, 2018, https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html, https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html.

Pomerleau, Mark. "Does Organizing Cyberspace Actually Ratchet up Potential for Conflict?" Fifth Domain, November 9, 2017. https://www.fifthdomain.com/dod/cybercom/2017/11/09/does-organizing-cyberspace-actually-ratchet-up-potential-for-conflict/.

Prier, Jarred. "The Command of the Trend:  Social Media as a Weapon in the Information Age." SAASS Air University, 2017. http://www.dtic.mil/docs/citations/AD1039253.

Qutb, Sayed. *Milestones*. Islamabad: Islamic Book Service, 2006.

Salmoni, Dr. Barak A, and Dr. Paula Holmes-Eber. *Operational Culture for the Warfighter: Principles and Applications*. Quantico, VA: Marine Corps University, 2008.

Satter, Raphael. “US Military Wives Threatened by Russian Hackers Posing as ISIS.” Fifth Domain, May 8, 2018. http://www.fifthdomain.com/dod/2018/05/08/us-military-wives-threatened-by-russian-hackers-posing-as-is/.

Satter, Raphael, Jeff Donn, and Justin Myers. “Russia Hackers Had Targets Worldwide, beyond US Election.” Fifth Domain, November 2, 2017. https://www.fifthdomain.com/civilian/2017/11/02/russia-hackers-had-targets-worldwide-beyond-us-election/.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.

Sheehan, Michael. *The International Politics of Space (Space Power and Politics)*. 1st edition. London: Routledge, 2007.

Slaughter, Anne-Marie. “International Relations, Principal Theories.” *Max Planck Encyclopedia of Public International Law*. Oxford University Press, 2011.

“SMA DESCRIPTION | NSI.” Accessed April 19, 2018. http://nsiteam.com/sma-description/.

Special Report. “Waging War with Disinformation.” *The Economist*, January 25, 2018. https://www.economist.com/news/special-report/21735479-power-fake-news-and-undue-influence-waging-war-disinformation.

Stevenson, David. “Cyber:  Changing the Landscape of Foreign Intervention in Democratic Elections.” SAASS Air University, 2017. http://www.dtic.mil/docs/citations/AD1039256.

Technology Quarterly. “Brain-Computer Interfaces.” *The Economist*, January 6, 2018.

Tocqueville, Alexis De. *Democracy in America*. Vol. 1. New York, NY: The Century Co., 1898.

Tucker, Patrick. “How US Special Operators Helped Take Down Joseph Kony’s Army with Tailored Messages - Defense One.” Defense One, October 17, 2017. http://www.defenseone.com/technology/2017/10/how-4-green-berets-took-down-joseph-konys-army-tailored-messages/141851/?oref=defenseone_today_nl.

———. “Policy and Will, Not Cyber Weapons, Are Missing in Action Against Russian Information Attacks.” Defense One. Accessed March 22, 2018. http://www.defenseone.com/technology/2018/02/policy-and-will-not-cyber-weapons-are-whats-missing-action-against-russian-information-attacks/146282/.

Tufekci, Zeynep. “It’s the (Democracy-Poisoning) Golden Age of Free Speech | WIRED.” WIRED, January 16, 2018. https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/.

Tyson, Neil deGrasse. *Space Chronicles: Facing the Ultimate Frontier*. 1 edition. New York, NY: W. W. Norton & Company, 2014.

United States. *Summary of the 2018 National Defense Strategy of The United States of America*. Accessed February 1, 2018. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

US Department of State. *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 - 87*. Washington D.C.: Bureau of Public Affairs, 1987. http://jmw.typepad.com/files/state-department---a-report-on-active-measures-and-propaganda.pdf.

US Joint Chief of Staffs. Joint Concept for Human Aspects of Military Operations, 2016.

Van Vleck, Jenifer. *Empire of the Air: Aviation and the American Ascendancy*. Cambridge, MA: Harvard University Press, 2013.

Vitkovskaya, Julie, Samuel Granados, and John Muyskens. "The Post's New Findings in Russia's Bold Campaign to Influence the U.S. Election." Washington Post. Accessed November 29, 2017. https://www.washingtonpost.com/graphics/2017/world/national-security/russia-hacking-timeline/.

Votel, Joseph, Charles Cleveland, Charles Connett, and Will Irwin. "Unconventional Warfare in the Gray Zone." National Defense University Press, January 1, 2016, 9. http://ndupress.ndu.edu/Publications/Article/643108/unconventional-warfare-in-the-gray-zone/.

Wendt, Alexander. *Social Theory of International Politics*. Cambridge Studies in International Relations 67. Cambridge: Cambridge University Press, 1999.

Williams, Brad D. "Narrative, Cyberspace and the 21st Century Art of War." Fifth Domain, January 22, 2017. http://www.fifthdomain.com/2017/01/22/narrative-cyberspace-and-the-21st-century-art-of-war/.

Winton, Harold R. "An Imperfect Jewel: Military Theory and the Military Profession." *Journal of Strategic Studies* 34, no. 6 (2011): 853–877.

Yarger, H. Richard. "Towards A Theory of Strategy:" Accessed April 15, 2018. http://www.au.af.mil/au/awc/awcgate/army-usawc/stratpap.htm.

Zegart, Amy. "The Tools of Espionage Are Going Mainstream." *The Atlantic*, November 27, 2017. https://www.theatlantic.com/international/archive/2017/11/deception-russia-election-meddling-technology-national-security/546644/.

Zi, Sun. *The Art of War*. Translated by Gary J. Bjorge. Fort Leavenworth, KS: Department of Military History, US Army Command and General Staff College, 2005.