Gray Zone Challenges: Optimizing Organizational Structures and Improving Cognition for DoD and the Interagency

A Monograph

by

Benjamin Nguyen Jehle
Federal Emergency Management Agency

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

2018

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
24-05-2018	Master's Thesis	June 2017-May 2018

4. TITLE AND SUBTITLE
Gray Zone Challenges: Optimizing Organizational Structures and Improving Cognition For DoD and the Interagency

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Benjamin Nguyen Jehle

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Operational Arts Studies Fellowship, Advanced Military Studies Program

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Gray Zone conflicts occur in areas where adversaries use a combination of small-scale tactical operations, operational environment ambiguity, and a wide array of communications mediums to deliver targeted narratives that advance their objectives while ensuring their activities do not meet the threshold for a US military response. The gradual, incremental nature of Gray Zone actions combined with the multiple levels, multiple time scales and multiple areas make assessing and responding to Gray Zone strategies challenging to recognize, understand, and then efficiently respond to. For the United States to recognize and potentially respond to Gray Zone strategies that place American interests or those of an ally at risk also requires a level of information sharing and collaboration that in most cases does not exist between departments, agencies, and allies targeted by Gray Zone actors. This study considers how DoD and the Interagency are currently organized to assess and respond to Gray Zone challenges. It discusses recommendations for how to improve how DoD and the Interagency are organized and where opportunities exist to improve both cognition of Gray Zone activities to shape or deter Gray Zone operations and when they require a response. Gray Zone competition requires a tailored approach that includes options from across the levers of diplomatic, information, military and economic powers that reflect a whole-of-government unified effort and make the United States response less predictable and more efficacious.

15. SUBJECT TERMS
Gray Zone, Information Operations, Interagency, Open Source Intelligence, Social Media, Cognition, Whole of Government, Strategic Communications, Unified effort.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Benjamin N. Jehle
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	(U)	47	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified			

Monograph Approval Page

Name of Candidate: Benjamin N. Jehle

Monograph Title: Gray Zone Challenges: Optimizing Organizational Structures and Improving Cognition for DoD and the Interagency

Approved by:

_____, Monograph Director
Dan Cox, PhD

_____, Seminar Leader
Jason A. Curl, COL

_____, Director, School of Advanced Military Studies
James C. Markert, COL

Accepted this 24th day of May 2018 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

Abstract

Gray Zone Challenges: Optimizing Organizational Structures and Improving Cognition for DoD and the Interagency, by Benjamin Nguyen Jehle, 46 pages

Gray Zone conflicts occur in areas where adversaries use a combination of small-scale tactical operations, operational environment ambiguity, and a wide array of communication mediums to deliver targeted narratives that advance their objectives while ensuring their activities do not meet the threshold for a United States military response. The gradual, incremental nature of Gray Zone actions combined with the multiple levels, multiple time scales, and multiple areas make assessing and responding to Gray Zone strategies challenging to recognize, understand, and then efficiently respond to. For the United States to recognize and potentially respond to Gray Zone strategies that place American interests or those of an ally at risk also requires a level of information sharing and collaboration that in most cases does not exist between departments, agencies, and allies targeted by Gray Zone actors.

This study considers how DoD and the Interagency are currently organized to assess and respond to Gray Zone challenges. It discusses recommendations for how to improve how DoD and the Interagency are organized and where opportunities exist to improve both cognition of Gray Zone activities to shape or deter Gray Zone operations and when they require a response. Gray Zone competition requires a tailored approach that includes options from across the levers of diplomatic, information, military and economic power that reflect a whole-of-government unified effort and make the United States response less predictable and more efficacious.

Contents

Acronyms

AI	Artificial Intelligence
AO	Area of Operations
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
CCIR	Commander's Critical Information Requirements
CJCS	Chairman Joint Chief of Staff
CMOC	Civil-Military Operations Center
CNA/CND	Cyber Network Attack/Cyber Network Defense
CNO	Cyber Network Operations
COG	Center of Gravity
COMINT	Communications Intelligence
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DIME	Diplomacy, Information, Military, and Economic(power levers)
DoD	Department of Defense
DoS	Department of State
EW	Electronic Warfare
HUMINT	Human Intelligence
I&W	Indications and Warning
IARPA	Intelligence Advanced Research Projects Activity
IC	Intelligence Community
IO	Information Operations
IW	Information Warfare
ISR	Intelligence, Surveillance, Reconnaissance

KLE	Key Leader Engagement
NDS	National Defense Strategy
NSC	National Security Council
NSS	National Security Strategy
OE	Operational Environment
OSI/OSINT	Open Source Intelligence
SC	Strategic Communications
SIGINT	Signals Intelligence
SM	Social Media
SO	Shaping Operations
SOCMINT	Social Media Intelligence
SOF	Special Operations Forces
TSC	Theater Security Cooperation
TA	Target Audience
USAID	United States Agency for International Development
USG	United States Government
WOG	Whole of Government

Illustrations

Introduction

The United States faces competition globally from states, non-state actors, insurgencies and other ideologically based groups who want to erode or diminish American influence and power. A strategy that enables a competitor to achieve its goals without triggering an American response is the very essence of a Gray Zone competitor. Gray Zone environments are challenging for the United States Government (USG) from a national security perspective to recognize or to deter. Gray Zone adversaries have shown that they could stay "below the radar" of the United States National Security apparatus as they pursue their goals and compete with the United States. Gray Zone actors are adept at finding opportunities to achieve their goals incrementally and under cover of ambiguity to challenge international law, influence local populations, and promote their agendas while avoiding the costs of challenging the United States.

A common theme when discussing the challenges of Gray Zone environments is that they require a whole of government approach to deter or respond to threats against the interests of the United States. JCS Publication 1-0 states that "military operations alone rarely resolve conflicts [including Gray Zone conflicts] and the United States will always [operate] from the perspective of a nation-state, whole-of-nation approaches where the military instrument of power sets conditions for victory."[1] Gray Zone actors, like conventional adversaries, have vulnerabilities that are exploitable within their interconnected political, military, economic, social, information, and infrastructure systems.[2] Gray Zone competitors may not be a state, or have the capability to present an armed threat but can still present a significant threat to international order and the interests of the United States. The 2018 *National Security Strategy* (*NSS*) and *National Defense Strategy* (*NDS*) both recognize that Gray Zone threats are more prevalent and present a challenge

[1] US Department of Defense, Joint Staff, Joint Publication (JP) 1-0, *Doctrine for the Armed Forces* (Washington, DC: Government Printing Office, 2017), I-6.

[2] Ibid.

for Department of Defense (DoD) and the Interagency and require a "whole of government" response.[3] Diplomatic and economic Gray Zone shaping operations can offer a viable way to achieve deterrence while avoiding a conflagration where a kinetic military response option is required to protect the interests of the United States or international order. Nevertheless, those options also require information and coordination between the Interagency and DoD to ensure decision-makers have an accurate picture of Gray Zone activity and there is a process to consider what options are best suited to each situation. The organizational structure and the size of the United States Federal Government create challenges in integrating and sharing information about Gray Zone environments. The organizational and decision-making barriers inherent in an organization so massive and segmented results in an overly complicated decision-making structure that lacks agility. Information systems in each department evolve to meet unique information requirements that complicate interoperability and may have restrictions on data sharing with other departments in the Interagency. The result is each part of the Interagency and DoD depends on information derived primarily from data sources within their department and with little relative information sourced from Interagency partners which in effect creates an echo chamber and leads to a form of organizational cognitive dissonance.

The consequences of a failure to integrate and synchronize operations between DoD, the Interagency and National decision-makers sub-optimize how the United States understands, deters, and responds to Gray Zone threats and may potentially erode American prestige and allies' confidence. DoD and its Interagency partners must be able to work together in a focused, collaborative way to understand how a Gray Zone actor is working across multiple domains in a comprehensive way where they aggregate and analyze disparate data from many sources to

[3] Donald J. Trump, "National Security Strategy of the United States of America," Whitehouse.gov, last revised December 2017, accessed January 2, 2018, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, 7-14; US Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: US Department of Defense, 2018), 1-7.

provide a complete operational picture. The lack of a comprehensive and integrated picture of a Gray Zone operating environment unnecessarily limits cognition and potentially wastes resources that may sub-optimize response options.

Purpose and Significance

Gray Zone adversaries operate in a space that is not just about proxy wars, disinformation, and propaganda campaigns, or operating criminal networks to target American economic or commercial interests. Gray Zone actors also target diplomatic, economic, and information vulnerabilities to influence populations and to erode programs and policies of the United States or international community. Revisionist powers like Russia and China have shown their willingness to use Gray Zone operations to support their strategies to challenge international order or to "correct" what they see as past wrongs while avoiding American military intervention. The Russian annexation of Crimea and ongoing operations in Ukraine is an example of Russia Gray Zone operations. An example of the Chinese approach to Gray Zone is their operations in the South China Sea where they openly thwart recognized boundaries and territorial waters codified under international treaties and law. They also use a "lawfare" approach to lay claim to the Spratly and Paracel Islands. China creates Air Defense Identification Zones that breach recognized neighbor state established Air Defense Identification Zones to lay claim to neighbor state airspace as well as placing sensors and offensive/defensive weapons in contested areas as an anti-access/area denial strategy to exert control over territory they view as historically Chinese. Both examples above use various methods and operations to implement a Gray Zone strategy, but they implement them diverse ways. Some actions are overt by design and help create a sense of legitimacy in the messaging themes and narratives used in strategic communication goals for both the international community and domestic audiences. Other actions rely heavily on technology to support Gray Zone operations where non-attribution and anonymity are essential to influence a

target population, to conduct disinformation operations, and to challenge the United States or a host country.

The ability of the United States to advance its national interests is dependent on the effectiveness of the USG in employing the instruments of national power to achieve national strategic objectives.[4] The underlying premise of this study is that Gray Zone adversaries rely on both technology and multifaceted operations to conduct Gray Zone operations confident that United States Interagency and DoD will not understand how, who, or why a Gray Zone actor is conducting operations nor what their operational intent aims to achieve. The Interagency partners who implement economic, diplomatic, and information levers of power sacrifice decision speed and course of action selection because they are not integrated or synchronized with the military command and control (C2) structure who will be essential in providing the security environment for the soft power tools that they implement. Overlaps or seams in authority breed poor response options and execution and are utterly devoid of any unity of action. The lack of situational awareness stemming from unintegrated systems across the USG leaves operational commanders and decision-makers with an incomplete picture and lack of context. The combination of a lack of a scalable, tailorable organizational structure that cuts across DoD and the Interagency focused on persistent hybrid threats, plus the lack of an integrated picture of the operational environment challenges how the United States understands, deters, and responds to Gray Zone threats. The United States becomes predictable, exploitable, and ineffective in countering Gray Zone actor narratives or adversary influence operations.

The other barrier for Gray Zone operations and potentially the easiest to address is the fact that every part of DoD and the Interagency has a unique system or process that while right for departmental situational awareness, is not interoperable or integrated into a more complete

[4] Trump, "National Security Strategy of the United States of America," 7-14; US Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, 1-7.

and holistic picture where Gray Zone exists. Failure to understand how a Gray Zone actor is operating in different areas or communication mediums sub-optimizes how the United States responds and leads to underestimation or overreaction to Gray Zone events. Decision makers lack context provided by merely integrating information contained in another Interagency system. That does not mean that the best or only solution is one that can fuse every data source into one integrated picture so a decision-maker in Washington, DC can decide what is proper for USG personnel in theater facing a Gray Zone challenge. It means that those organizations who are collaborating understand and respond to Gray Zone threats have a way to visualize and understand data from multiple sources that show contextual and human terrain information so that the supported entity in the theater can respond quickly and with relevance. Gray Zone data and information must be available to National-level decision makers who can assess and craft strategic messaging themes or present US response options to the National Security Council when a more holistic picture of what a Gray Zone actor is doing calls for a response.

The process to collect, analyze, evaluate, and provide anticipatory decision support to decision-makers for Gray Zone environments portends a whole-of-government effort using a broad array of information types that will need processes and tools to extract meaningful intelligence to meet the optimization goals described above. Social media and social media intelligence, artificial intelligence, big data analytics, and other tools that offer a more in-depth understanding of the constructs of social fragmentation may inform not only shaping operations but can also potentially give meaningful information on the efficacy of friendly operations to counter Gray Zone competitors. Social networks provide a social-cultural context that traditional communication medium analysis cannot provide and may be critical in finding and interacting with important local influencers. Analytic tools capable of assessing and processing open source data (legacy media, internet news feeds, RSS), social media networks, and messaging applications are essential in building systems capable of recognizing adversary Information Operations (IO) where deception and counter-narratives affect the local population. Analytic

focus that incorporates data from the information environment and gives context to enhance cognitive awareness for decision-makers also enables increased decision space and the possibility for more options to respond. Another barrier for dominating Gray Zone competitors is in the information lever of power. Gray zone adversaries focus on creating counter-narratives to US messaging and policy and use a mix of targeted messaging, disinformation, propaganda, and physical events to influence local populations that are the target of operations. Effective Strategic Communication is essential to deliver an overarching message for the Interagency and to give a unifying message across the enterprise. Strategic Communications tools span the breadth of government and are an important lever of power in the DIME paradigm.

This study will focus on two fundamental barriers that the United States federal Interagency and DoD faces when responding to Gray Zone adversaries: organizational structure and the challenges of creating a complete and shared understanding of the operational environment. The US military is organized to fight conventional wars against conventional opponents. The new *National Defense Strategy* released in mid-January 2018 codifies that primary focus, and that American military power is focused on dominating any adversary in a conventional battle. However, the *NDS* also recognizes that Gray Zone threats exist and are becoming more prevalent and dangerous as technology enables a broader range of actors to challenge established international order. Revisionist powers like Russia and China have the ability and resources to challenge the United States in every domain but also understand what it means when the United States goes to war. The same is not true for non-state actors who see Gray Zone operations as an equalizer to threaten the most powerful nation on earth while expecting the minimal risk of retaliation. The culture of the United States and its government has historically been binary about how they function in either war or peace and have not had to consider the reality posed by Gray Zone threats where a persistent state of conflict exists. This study will analyze existing United States Federal Government assessment capabilities, tools, processes, and authorities used today and shows where the potential gaps and seams exist that may limit

cognition or complicate the right choice of response options. This research then offers potential solutions to improve and optimize anticipatory cognition of Gray Zone environments, improved decision speed, and where future development may optimize Interagency understanding and response options to Gray Zone threats.

Methodology

The methodology and research design that this project uses is to define what a Gray Zone operational environment is and what attributes create challenges in developing cognition for operational level and strategic level decision-makers as a precursor to action or response. Three broad focus areas then follow in a chronological and theme-based construct starting with historical examples of Gray Zone operations to illustrate how both national policy and military doctrine have evolved. The next section of the study focuses on current Gray Zone conflicts and the proliferation of technology coupled with a dynamic information environment that eliminates barriers for states and non-state actors to challenge the United States in ways that did not exist before the end of the 20th century. That ability to challenge the United States while not crossing a reactionary redline is an essential component for decision makers to understand. An element of predictability for the United States about how it will respond to Gray Zone threats highlights why DoD and Interagency cognition and the ability to coordinate and reframe US responses across the spectrum of political levers of power is crucial in defeating Gray Zone competitors. This paper briefly discusses the organizational structures and the bureaucratic process that enables collaboration and cooperation across the whole of government to align and synchronize. The goal is to end barriers to cognition, and uncoordinated processes which sub-optimize response options and potentially erodes US prestige.

The last section is focused on cognition and how to bring new tools and information to the DoD and Interagency effort to better understand Gray Zone environments and to achieve better integration of a wider range of data sources and information. DoD and Interagency

collaboration in dominating the information environment, reinvigorating the art of Strategic Communication, and creating agile response options for counter-narratives can be valuable when assessing the efficacy of both soft and hard power tools to mitigate or marginalize Gray Zone influence operations.

There are limitations to this study by design. This does not discuss specific capabilities and limitations due to the security requirements that this study contain no classified information. Additionally, open and unclassified sources for information and decision support systems used by federal departments with authorities or responsibilities for coordinating or implementing levers of national power (diplomatic, information, military, economic) are not fully discoverable in unclassified sources. Lastly, while it is evident that technology is the great equalizer that removes barriers to competition by Gray Zone actors, technology is also a primary source of vulnerability for both the United States and its adversaries. The vulnerability of information systems, infrastructure and anything connected to the internet, also known as the Internet of Things (IoT) represents a substantial threat and is very much part of the tools used by Gray Zone actors to support their operations but are outside the scope of this study.

Literature Review

Defining the Gray Zone Operational Environment

Gray Zone is a relatively new term in both defense and diplomatic circles, but it has quickly become a favorite way to label adversarial maneuvers short of war. Gray Zone becomes a term for anything that is amorphous and ambiguous and while there may be some press reporting, does not rise to the level of concern that requires military action. The imprecise use of what constitutes a Gray Zone combined with the cultural norm of either being in conflict or peace creates a cognitive bias in not being able to see that a third condition exists. The third condition and one closest to reality today is that even when the United States is not actively engaged in

conventional war, nation states or their proxies are still actively seeking to expand territory, to promote their political ideology, or to surreptitiously challenge international norms.

Policy-makers, strategic planners, and the Intelligence Community (IC) have all tried to describe or categorize events that do not fit into traditional definitions of behaviors or actions that may signal military or diplomatic competition. This is the Gray Zone. Being precise in defining a Gray Zone is not just an academic exercise to describe the ambiguity and uncertainty that is part of all conflict. Being precise helps define the crucial distinctions that make Gray Zone environments challenging and why winning in the Gray Zone will need a whole of government approach. Scholar and strategic policy expert Hal Brands summarized the need for a precise definition of Gray Zones noting that, "Gray Zone conflicts are not synonymous with "irregular War" or "Military Operations other than war (MOOTW) [and it] is the intent, not the means, that primarily distinguishes Gray Zone conflicts from other types of conflict. Gray Zone cannot mean everything if it is to mean anything."[5] There is a litany of terms that others associate with Gray Zone conflicts such as proxy warfare, salami-slicing, coercive strategies, and escalation dominance that all sound like they may fit into a Gray Zone category but fail to recognize the underlying intent of the action.[6]

Having described what Gray Zone environments do not include, then what are the kinds of operations or events that meet the "intent" clause? The simplest definition is that a Gray Zone is "the purposeful application of multiple elements of power—information, economic, military, political—to achieve objectives in ways that exceed the threshold for normal competition yet fall below the level of major interstate war."[7] That is not a Chairman Joint Chief of Staff Joint

---

[5] Hal Brands, "Paradoxes of the Gray Zone," *Foreign Policy Research Institute*, last revised February 5, 2016, accessed August 16, 2017, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

[6] Adam Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," *War on the Rocks*, last revised December 15, 2015, accessed September 29, 2017, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense.

[7] National Intelligence Council, "Foreign Approaches to Gray Zone Conflicts," accessed September 25, 2017, http://nsiteam.com/foreign-approaches-to-gray-zone-conflicts/.

Publication definition because there is no existing JCS publication or doctrine for Gray Zone operations. That definition is adequate but fails to acknowledge the complexity of building the underlying essential elements of information that will drive cognitive awareness for the USG Interagency responsible for implementing national security strategy. The Strategic Multi-Layer Assessment Program in support of USSOCOM constructed a more precise and comprehensive definition of Gray Zone to facilitate the development of operational level planning and response strategies. SOCOM plays a significant role for DoD in responding across the entire spectrum of military response options from conventional war to training partner military forces and is well suited to be a leader in Gray Zone environments. The output of the Strategic Multi-Layer Assessment report adds much-needed granularity to the Gray Zone definition:

> The Gray Zone is a conceptual space between peace and war, where activities are typically ambiguous or cloud attribution and exceeds the threshold of ordinary competition yet intentionally fall below the level of large-scale direct military conflict. Gray Zone Strategies [include] a series of actions by a state or non-state actor that challenge or violate international customs, norms, and laws for pursuing one or more broadly-defined national security interests without provoking direct military response (e.g., Challenging common understandings, conventions, and international norms while stopping short of clear violations of international law; employing violations of both international norms and laws in ways intended to avoid the penalties associated with legal violations; states using violent extremist organizations (VEOs) and non-state actors as proxies in an effort to integrate elements of power to advance particular security interests). In most cases, once significant, attributable coercive force has been used, the activities are no longer considered to be in the Gray Zone but have transitioned into the realm of traditional warfare. While Gray Zone activities may involve non-security domains and elements of national power, they are activities taken by an actor to gain some broadly defined security advantage over another.[8]

This expanded and more precise definition of the Gray Zone is informative in focusing on the unique and challenging elements of understanding how entities using a Gray Zone strategy may operate either covertly or overtly through economic influence, information control and propaganda, political influence, and social discontent to achieve their goals, while not breaching red lines that would cause direct military action.

[8] Belinda Bragg, *Gray Zone Conflicts, Challenges, and Opportunities: Integration Report* (Arlington, VA: National Security Innovations, 2017), 5.

Evolution of Gray Zone Competition

Gray Zone strategies and conflicts are not a 21st century invention. The Cold War between the Soviet Union and the West that dominated the political and military landscape over a forty-five year period in the last half of the 20th century easily meets the definition of a Gray Zone conflict. Much of the Cold War focused on political ideology and competition in the economic and military sphere (thus proving each sides' political ideology as superior). It also involved operations that focused on maintaining a degree of uncertainty and ambiguity including the use of state and non-state actors in proxy wars.[9] The Cold War maybe most associated with propaganda, misinformation campaigns, military and operational deception and the use of strategic messaging as a way to influence the opposing side or to create doubt while remaining under the threshold of open conventional warfare or worse, nuclear war. European powers faced the same kinds of Gray Zone conflicts as precursors to both World War I and II where gradual and coercive operations disguised by ambiguity and the inability to piece together what was happening and by whom eventually led to conventional military conflict and a major conflagration.[10] Suitable examples of the United States using a Gray Zone strategy to compete with adversaries but structured to avoid military confrontation to achieve national or military objectives are well known. Operations such as the Bay of Pigs in Cuba (1961) to depose Fidel Castro, support of the Contras in fighting the Nicaraguan Sandinistas (1979 to 1990), and American weapons and financial support to the Afghan Mujahideen during the Soviet invasion of Afghanistan (1979 to 1989)[11] are good examples.

---

[9] Joseph L. Votel, Charles T. Cleveland, Charles T. Connett, and Will Irwin "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80, no. 1 (2016): 101–109.

[10] Nicholas D. Wright, *From Control to Influence: Cognition in the Gray Zone,* Report for the Pentagon Joint Staff Strategic Multilayer Assessment Group (Birmingham, UK: Institute for Conflict, Cooperation and Security, University of Birmingham, 2017), 1.

[11] Ibid., 35-36.

21st Century Gray Zone Operational Environment Challenges

The most significant factor that has changed who can be a Gray Zone actor is technology. The Internet and the proliferation of social media platforms that enable instantaneous communication and data services like video streaming have enabled anyone with necessary technical skills and the intent to influence an audience to assume a role as a Gray Zone actor. For technologically advanced groups or states who use Gray Zone strategies to challenge international order without attribution, the Internet and social media in particular, offer an attractive way to communicate and influence audiences at no cost and with almost no risk. Social media enables Gray Zone actors or their proxies to deliver disinformation and counter-narratives that resonate with local audiences. The use of technology to support Gray Zone operations varies widely. The Internet and encrypted communications using messaging apps are valuable recruiting tools and vital propaganda channels for groups like the Islamic State and Al Qaeda. The PRC, in contrast, is less enthusiastic about using social media channels to support their Gray Zone activities but relies heavily on technology to support their narratives related to foreign countries who challenge or operate within what they consider to be their economic exclusion zone. Both Russia and Iran represent states who are technologically advanced and use the Internet, social media, and other cyber activity to their advantage. The challenge for the United States and its allies is in recognizing when social media or technology is part of a Gray Zone strategy. While companies in the United States created many of the best-known and most popular social media sites, there are many hundreds more social media and applications hosted in countries like Russia and China that are popular for indigenous populations but remain unknown to DoD or Interagency analysts trying to understand Gray Zone activities in progress.

The gradual, incremental nature of Gray Zone actions combined with the multiple levels, multiple time scales, and multiple areas make assessing and responding to Gray Zone strategies challenging to recognize, understand, and then efficiently respond to. For the United States to recognize and potentially respond to Gray Zone strategies that place American interests or those

of an ally at risk also requires a level of information sharing and collaboration that in most cases does not exist between departments, agencies, and allies targeted by Gray Zone actors. The ability to understand Gray Zone strategies requires a way to collect, analyze, and visualize multiple types of Gray Zone tactical actions and to assess those events both as discrete events and then how those events fit within a broader regional context to create a holistic picture of an adversary's actions. Social media and the Internet provide our adversaries with unlimited global access to their intended audiences, while legal and policy issues paralyze the USG.[12] Even though the United States is one of the most technologically advanced countries in the world, it follows international law which constrains it, by design from using the internet and technology to influence or provide propaganda or disinformation to other countries.[13] Laws do not restrict states and nonstate actors participating in Grey Zone activities from using technology for nefarious reasons.

For example, in the Russian view, nonmilitary measures of warfare include economic sanctions, disruption of diplomatic ties, and political and diplomatic pressure. The Russians see information operations as a critical part of nonmilitary measures. They have adapted from well-established Soviet techniques of subversion and destabilization for the age of the Internet and social media. Russia has a very different view than the United States, where information operations are a continuous activity, regardless of the state of relations with any government. For the United States, information operations are associated with military operations prior to and in conjunction with combat operations (phase 2 through phase 4 depicted in figure 4 below). The distinction is important because, for Russia, information operations is a standard and constant

[12] RAND Corporation, *The Weaponization of Information: The Need for Cognitive Security,* Testimony of Rand Waltman before the United States Sentate Committee on Armed Services Subcommittee on Cybersecurity (Santa Monica, CA: RAND Corporation, 2017).

[13] Michael J. Mazarr, Mastering the Gray Zone: Understand a Changing Era of Conflict, United States Army War College Strategic Studies Institute. December 2015, accessed November 12, 2017, https://ssi.armywarcollege.edu/pdffiles/PUB1303.pdf, 108.

military activity, while the United States views information operations as a shaping tool to be used in conjunction with combat. Russian General Valery Gerasimov described a new approach to warfare in a 2013 article in *Military-Industrial Courier*. In it, Gerasimov argued for a new Russian strategy where his country could employ various resources so that "a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."[14] Figure 1 summarizes General Gerasimov's doctrine where it is clear that nonmilitary measures are more prolific and cross much more of the conflict spectrum than military operations do.

[14] Jahara Matisek and Ian Bertram, "The Death of American Conventional Warfare: It's the Political Willpower, Stupid," *The Strategy Bridge*, last revised November 5, 2017, accessed December 1, 2017, https://thestrategybridge.org/the-bridge/2017/11/5/the-death-of-american-conventional-warfare-its-the-political-willpower-stupid.

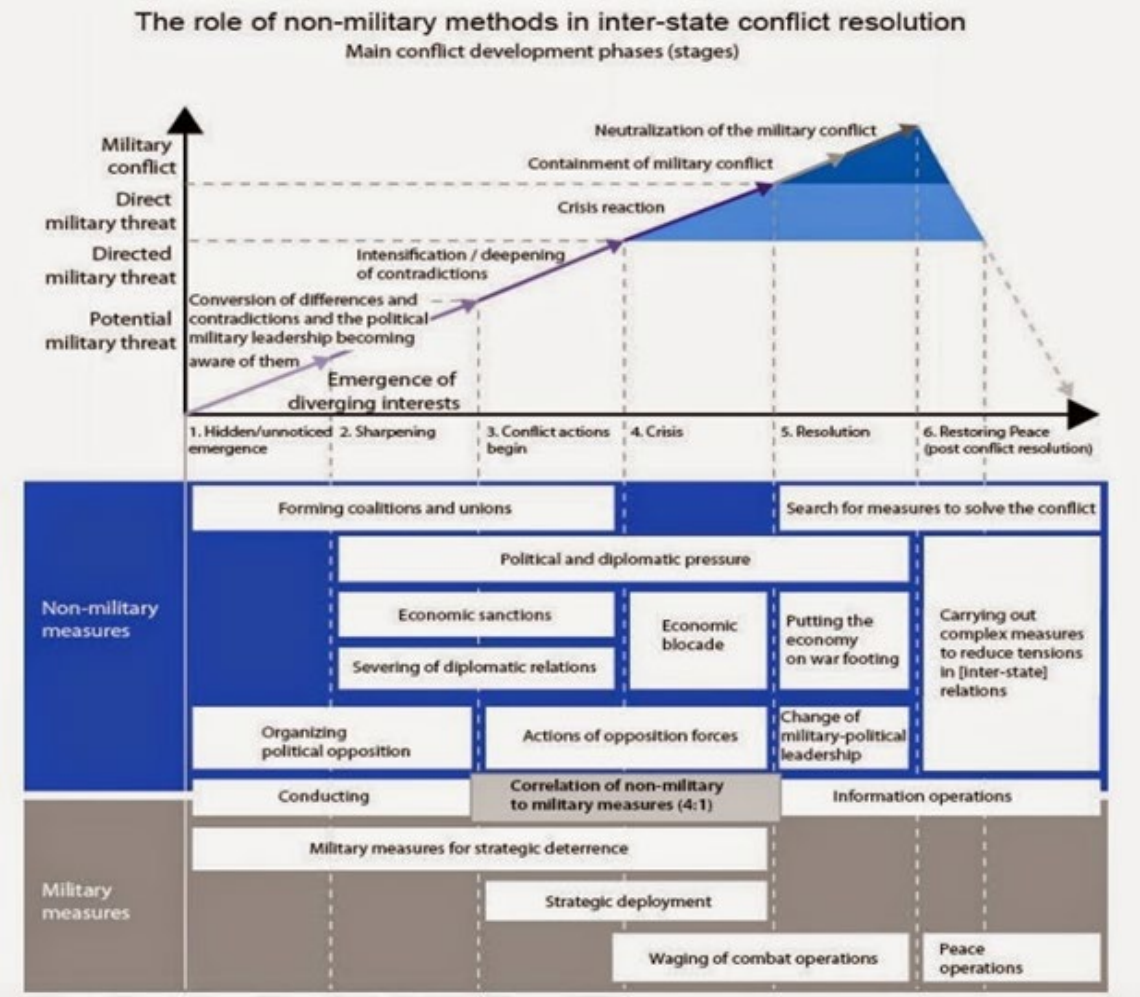

Figure 1. Russian General Gerasimov Doctrine on defeating enemies through a "combination of political, economic, information, technological, and ecological campaigns." Graphic from Gerasimov article in Voyenno-Promyshlennyy Kurier, 26 February 2013, translated by Charles Bartles, "Getting Gerasimov Right", Charles Bartles, Military Review, Jan-Feb 2016, 35.

It is the character and nature of Gray Zone conflicts that enables ambiguity across multiple domains that is crucial for those actors looking to carry out their objective through gradual, coercive incrementalism.[15] Nicholas Wright posits that the "Five multiples of a Gray

[15] Peter Pomerantsev, "Inside the Kremlin's Hall of Mirrors," *The Guardian*, April 9, 2015, accessed September 25, 2017, https://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology.

Zone" drives complexity and makes developing a response problematic in his meta-analysis of past Grey Zone events. Wright names the five multiples as:

> 1. *Multiple levels* where Gray Zone actors can influence including the state level, population level, and at the non-state actor level.
>
> 2. *Multiple domains* including military, information, economic, and cyber cut across multiple societal levels.
>
> 3. *Multiple timeframes* including near-term and long-term operations that may appear unrelated or unsynchronized.
>
> 4. *Multiple audiences* including host nation population, allied or partner nation perceptions, and third-party perceptions.
>
> 5. *Multiple interpretations* means that ambiguity is the essence of Gray Zone operations and enables multiple interpretations and narratives to develop. Ambiguity provides an extra layer of uncertainty, complicates risk assessment and is a critical factor in conflagration to crisis escalation.[16]

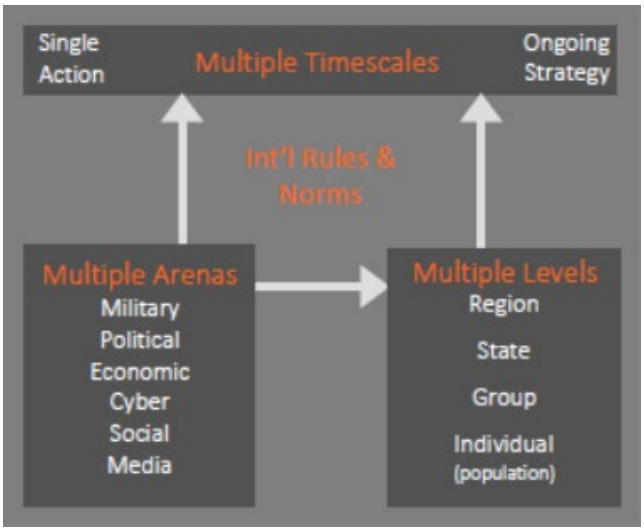

Figure 2. Nature of the Gray Zone. Nicholas D. Wright, *From Control to Influence: Cognition in the Gray Zone,* Report for the Pentagon Joint Staff Strategic Multilayer Assessment Group (Birmingham, UK: Institute for Conflict, Cooperation and Security, University of Birmingham, 2017), vii-viii.

[16] Wright, *From Control to Influence: Cognition in the Grey Zone.*

Secretary of Defense Mattis summed up Gray Zone challenges in his executive summary of the 2018 national defense strategy where he wrote:

> Some competitors and adversaries look to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion). These trends, if unaddressed, will challenge our ability to deter aggression. New technologies include advanced computing, 'big data' analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future. It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.[17]

Organizational Structure Barriers in Gray Zones: Who is in Charge?

A common theme to hear from USG senior leaders when discussing Gray Zone conflicts is that a "whole of government" approach is essential to recognize and respond to protect United States National Security interests. However, what does that mean? Are these leaders saying that Cabinet Level leaders have created an organization that is collaborative, integrated, and able to direct Gray Zone operations across the spectrum of American levers of power? Hardly. The most critical organizational obstacle in achieving a highly integrated and wide-ranging effort is that there is no common chain of command short of the President, no capability for strategic planning for the whole government effort, and no established structure for management and coordination of implementation across the federal government.[18] DoD is an integral part of providing Gray Zone response as is the State Department and many other organizations. Gray Zones, by definition, are not inherently situations where a military hard power option is the preferred choice

[17] US Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America,* 3.

[18] International Security Advisory Board (ISAB), *Gray Zone Conflicts* (Washington, DC: US Department of State, 2017), 6.

and therefore diplomacy under the purview of the State Department is often the primary method of resolving issues.

The question then is who or what entity handles leading a whole of government effort, what organizations contribute, and how do they make decisions to defeat competitors in Gray Zone environments? At the national level, no single organization or structure manages Gray Zone environments although there are plenty of opinions on how to organize for these security threats. The Department of Defense reorganized under Goldwater-Nichols in 1986 as a response to a series of operations that showed the world that the United States military could not effectively work as a joint fighting force. The effect of Goldwater-Nichols has been profound in the way DoD is organized to conduct war and how the Geographic Combatant Commanders (GCC) are supported to execute responsibilities codified in the Unified Command Plan (UCP).[19] Joint Planning doctrine also gives options for GCC's to respond to regional events to deter an actor from taking further action or in cases where an adversary has threatened or conducted aggressive behavior, describes how DoD will respond to those events. JCS Pub 5-0 states that the DoD executes flexible deterrent operations and flexible response options on order and give scalable options to respond to a crisis [as] adaptive military options for SecDef or the President to deter or respond to a crisis. Both provide the ability to escalate or de-escalate based on continuous assessment of an adversary's actions and reactions.[20]

While the Combatant Command model has been successful in fighting wars or responding to events where DoD has a role to play, the same model can pose organizational challenges in Gray Zone environments. The power to own and control all aspects of a theater of operations can also become a constraint when faced with an adversary who can operate in

---

[19] Andrew Feicker*, The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, Congressional Research Service (Washington, DC: Library of Congress, January 3, 2013) accessed October 9, 2017,https://fas.org/sgp/crs/natsec/R42077.pdf, 1-2.

[20] US Department of Defense, Joint Staff, Joint Publication (JP) 5-0, *Joint Planning* (Washington, DC: Government Printing Office, 2017), II-27.

multiple places and domains that cross GCC boundaries. Senator John McCain, who serves as the Senate Armed Services Committee Chairman posited that the Department of Defense must be able to "strategically integrate [and] develop strategies to integrate military power globally to confront a series of threats, both states, and non-state actors, all of which span multiple regions of the world and numerous military functions."[21] Gray Zone actors can present a challenge to the rigid GCC structure GCCs' control forces assigned and appointed to them and the territory inside their AOR boundaries. Consider a Gray Zone theater where Russia was believed to be using Gray Zone strategies that threatened the interests of the United States. Russia is a massive country where multiple Combatant Commands have equities including EUCOM (Eastern Europe, Baltic States, and Balkan States), PACOM (Eastern Russia), CENTCOM (states between the Persian Gulf and Southern Russia), EUCOM and NORTHCOM for Arctic Operations, and STRATCOM and CYBERCOM for space and cyberspace. Each of those GCCs and the Functional Combatant Commanders vie for resources and authorities to conduct operations under their Title 10 responsibilities are supported. In a Russia scenario, which Combatant Command is the supported commander? If the President or the National Security Council decides the initial plan is to pursue a diplomatic solution first along with economic and informational strategies to compel Russia to behave, does it matter who the supported Combatant Command is? A former Combatant Command J5 stated, "You have got to tie all those activities together [for cross domain/cross AOR Gray Zone threats,] [that] cannot be done at the regional combatant commander level."[22] Since the Chairman Joint Chief of Staff is not in an operational role, the Secretary of Defense, by default, becomes the integrator and referee with the requisite authority to arbitrate and coordinate

[21] McInnis, Kathleen J. Goldwater-Nichols at 30: Defense Reform and Issues for Congress. Washington, DC: Congressional Research Service, 2016. Page 21.

[22] Frederick S Brundick and Josh Dehlinger, "IChart: A Tool for Visualizing and Managing Organizational and Force Structure Data" (Presentation, 16th International Command and Coltrol Research and Technology Symposium, Quebec, Canada, June 21-23, 2011), accessed February 11, 2018, http://www.dtic.mil/dtic/tr/fulltext/u2/a547388.pdf.

between the Combatant Commands. It becomes a top-down solution where the SecDef makes allocation decisions and referees Combatant Command disagreements.[23] Former Secretary of Defense Ashton Carter highlighted the problem with this model when he stated, "increasingly complex security environments and a decision chain that cuts across the combatant commands only at the level of the Secretary of Defense [does not] posture us to be as agile as we could be."[24]

The current Chairman of the Joint Chiefs, General Dunford, has posited that it is the failure to understand that the war or peace binary condition does not recognize reality where Gray Zone actors are a constant, persistent threat who occupy the space between war and peace.[25] General Dunford is critical of the traditional phasing plan as well. Regarding Gray Zone threats specifically, he stated that:

> [He] does not find the current phasing construct for operational plans particularly useful right now. If you think about it, we bend authorities and capabilities according to where we think we are in a phase. I asked all the combatant commanders in your area of responsibility, what phase is your adversary in? . . . and consistently the combatant commanders said: Well, I think our adversary is in phase 2, or our adversary is in phase 2 ½. I call that competition with a military dimension short of phase 3 or traditional conflict including employment of cyber, unconventional capabilities, space capabilities, information operations that are not associated with what we would call phase zero shaping.[26]

---

[23] Sydney J. Freedberg, "Joint Staff Must Boost Global Coordination; No New Powers Needed: J5," *Breaking Defense*, last updated April 27, 2017, accessed November 30, 2017, https://breakingdefense.com/2017/04/joint-staff-must-step-up-global-coordination-no-new-powers-needed-j-5/.

[24] US Department of Defense, "Remarks on 'Goldwater-Nichols at 30: An Agenda for Updating,'" April 5, 2016, accessed January 4, 2018, https://www.defense.gov/News/Speeches/Speech-View/Article/713736/remarks-on-goldwater-nichols-at-30-an-agenda-for-updating-center-forstrategic/.

[25] Colin Clark, "CJCS Dunford Calls for Strategic Shifts: 'At Peace or At War is Insufficient,'" *Breaking Defense,* September 21, 2016, accessed October 17, 2017, https//breakingdefense.com/2016/09/cjcs-dunford-calls-for-strategic-shifts-at-peace-or-at-war-is-insiffiecient/.

[26] Paul Scharre, "American Strategy and the Six Phases of Grief," *War on the Rocks*, October 6, 2016, accessed December 9, 2017, https://warontherocks.com/2016/10/american-strategy-and-the-six-phases-of-grief/.

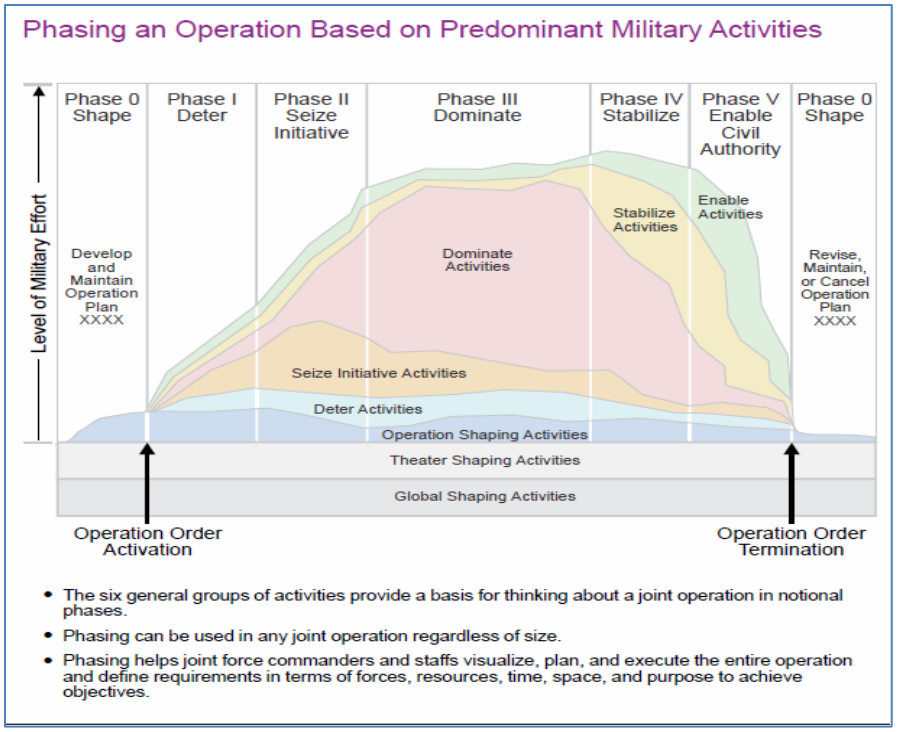

Figure 3. Phasing an Operation Based on Military Activity. Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, January 2017), V-8.

Goldwater-Nichols removed the Joint Chiefs from the operational control of forces, so Chairman Joint Chief of Staff has limited ability to coordinate cross-domain/cross-AOR issues. Chairman Joint Chief of Staff controls apportionment and assignment of forces and therefore does have influence with the GCCs from a resources perspective including validation of Requests for Forces (RFF), assigning roles and responsibilities for the CCDRs outlined in the Unified Command Plan and Forces for (Allocation and Apportionment), and in Global Force Management (GFM) as outlined in figure 4 below.

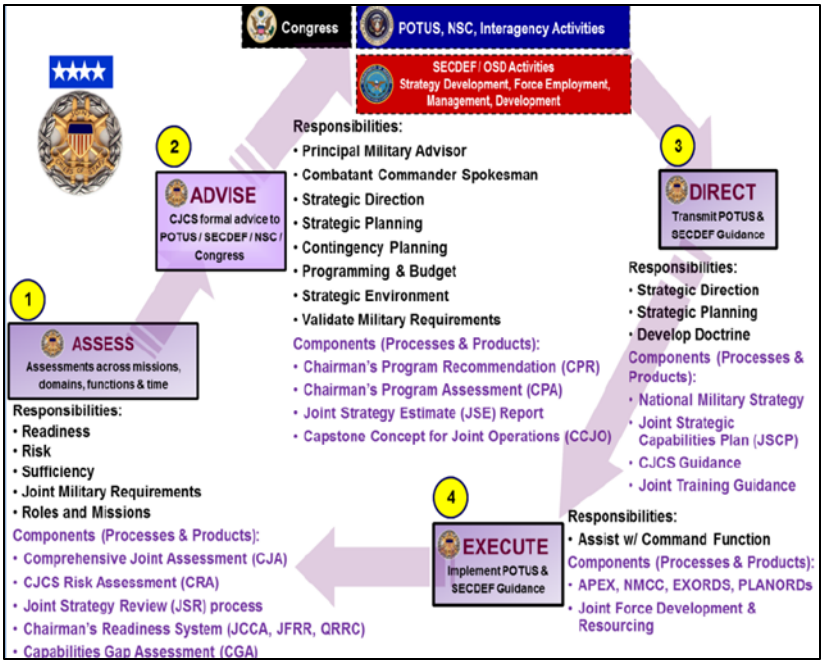

Figure 4. Chairman Joint Chief of Staff Roles, Responsibilities, and Associated Components. Chairman of the Joint Chiefs of Staff, CJCSI 3100.01C, *Joint Strategic Planning System (JSPS)* (Washington, DC: Government Printing Office, 2015), A-1.

The view from an Interagency perspective at a strategic level is different regarding the best way to organize for response to Gray Zone threats. The Department of State (DoS) International Security Advisor Board believes that, "the military cannot be expected to deliver alone even on all the security tasks [associated with Gray Zones]. Often law enforcement, "rule of law" assistance, intelligence support, border control, and other critical–but non-military–security fields will be more critical [and] because the conflict is (mostly) non-military, DoD is not well-suited to be in operational charge overall."[27] Instead, DoS believes there should be a civilian-led structure for planning and management to execute United States counter-GZ activities within a centrally determined strategy and capable of managing the difficult task of coordinating military and civilian actions in the field.[28]

[27] International Security Advisory Board (ISAB), *Gray Zone Conflicts* (Washington, DC: US Department of State, 2017), 7.

[28] Ibid.

The Secretary of State, Secretary of Treasury, and Secretary of Defense are all statutory members of the National Security Council.[29] The State Department is also responsible for conducting diplomacy on behalf of the United States which is generally the preferred course of action when resolving disputes with other countries in the international community. It is State's role in international diplomacy and its organizational structure of diplomatic missions, embassy staff, and Foreign Service corps that supports those who believe State is better positioned to lead Gray Zone responses than DoD. The diplomacy mission plus the fact that DoS has its own bureau for intelligence, bureau for political affairs, bureau of conflict and stabilization operations, bureau of counterterrorism and the newly established Global Engagement Center (GEC) makes it is easy to see why DoS might believe they should have primacy for Gray Zone theaters. The Global Engagement Center was established in April 2016 pursuant to Executive Order 13721 and codified into law by Congress in the Fiscal Year (FY) 2017 National Defense Authorization Act (NDAA), which defined its mission as being to "lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[30] According to DoS, the GEC operates as a "forward-looking, innovative organization that can shift focus quickly to remain responsive to agile adversaries. The GEC leverages data science, innovative advertising technologies, and top talent from the private sector. With detailees from across the Interagency, the GEC coordinates messaging efforts to ensure they are streamlined to eliminate duplication."[31]

[29] Whitehouse.gov, "National Security Council," last updated December 1, 2017, accessed December 12, 2017, https://www.whitehouse.gov/nsc/.

[30] Ibid.

[31] Ibid.

What the DoS does not have is a regional-level civilian institution, comparable to a GCC, that can direct regional-level activities.[32] The fiscal climate in the United States in an era of 20 trillion dollar debt is a major obstacle for State to create a parallel civilian organization to the DoD GCC structure. Others see a potential for integrating a robust civilian management element with the military's regional CCMD structure, because of the need for close coordination between the two lines of effort.[33]

Chain of Command-Strategy–C2-Unity of Effort

There must be a clear, unambiguous structure that provides a clear chain of command for how operations will be conducted in whichever organizational structure the President decides to implement to address Grey Zone adversaries. The entity charged with deterring and responding to Gray Zone competitors needs to select a strategy that will inform and drive national-level decision making, planning across the USG, and finally execution of operations across the levers of power to compel Gray Zone actors to cease activities. Real strategy requires exacting depictions of the essential problem and a clear choice among competing solutions to guide the means the United States develops and employs. Most importantly, the organizational structure and strategy must result in unity of effort across the entire DoD and Interagency structure.[34] There are lessons from the seventeen plus year conflict in Afghanistan, Iraq, Yemen and other hot spots throughout the broader Middle East and North Africa (MENA) theater of operations that are informative about organizational structures and command and control (C2) required to compete and be successful when faced with an adversary who uses many of the same strategies as a Gray Zone actor. Adversaries such as the Taliban, al Qaeda and the Haqqani network who control the

[32] Whitehouse.gov, "National Security Council," last updated December 1, 2017, accessed December 12, 2017, https://www.whitehouse.gov/nsc/.

[33] Ibid.

[34] Richard Hooker and Joseph J. Collins, *Lessons Encountered: Learning from the Long War* (Washington, DC: National Defense University Press, 2015), 9-10.

much of Afghanistan-Pakistani border region, and more recently Islamic State in Western Iraq and Syria operate in a similar manner where multifaceted operations combined with efficient use of technology make them a persistent and lethal threat to United States national security interests worldwide.

General Stanley McChrystal was the JSOC commander in Afghanistan and Iraq from 2003 through 2008 during a time when there was a significant resurgence of terrorism challenging the then United States-dominated fight for territory. In numerous interviews and in his book, *Team of Teams: New Rules of Engagement for a Complex World*, General McChrystal discussed how organizational structure and the C2 that connects the organization can either be a strength or an impediment to success, particularly in circumstances where a commander is faced with an elusive, innovative, and agile adversary. His ideas about empowering organizations that require speed and agility are informative for Gray Zone operations. For example, focussing on enabling "doers" by getting the right information to the right people who are making tactical decisions vice concentrating on feeding information up to decision-makers in a top-down hierarchical structure is an important point. Resources (time, money, people, effort) spent arguing about who is in charge of Gray Zones does nothing to support DoD and the Interagency. General McChrystal's formula in developing robust communications and information sharing processes that keep the organization synchronized is another key lessons learned. They may appear to be unachievable when faced with sharing information between all the federal government departments and their information silos, but it is also clear to senior decision-makers and organizations who execute Gray Zone operations that failure to share information and keep everyone synchronized is a sure way to fail against an adversary capable of capitalizing on any miscommunication. He also realized quickly that promoting opportunities for people who are from different agencies or departments to work face-to-face so they develop a shared consciousness and emotional ties are critical in building effective teams able to operate

together.[35] Leaders need to worry less about controlling information flow and more about identifying impediments to progress that jeopardize the mission.

The current decision-making framework for Gray Zone environments does not enable the shared consciousness General McChrystal knows is necessary to succeed in complex environments. There is no single person in charge, and organizations compete rather than cooperate. This creates stove piped diplomatic, military and intelligence products for different chains of command and then rely on complex Washington decision-making procedures. It often produces confusion, mixed signals, and slow reactions.[36] It becomes the opposite of unity of effort for an array of contributors who have a role in Gray Zone environments. Managing across organizational boundaries is a complex skill that requires, among other things, working hard to build relationships with counterparts, understanding the decision-making styles of superiors, and developing trust within top leadership circles. As Hooker et al so eloquently state in their analysis of United States operations over the past two decades;

> Insufficient unity of effort is not just a 'civilian' or Interagency problem, and it is a challenge for the Pentagon and military operations. DoD is susceptible when leaders responsible for war planning, postwar planning, war resourcing, or command and control of military forces in the field suffer from a 'strategy formulation and execution problem.'[37]

Good decision making requires a range of views, but once a decision has been made, the entire organization needs to implement the decision with a unified effort both vertically and horizontally. Vertical unity of effort is the C2 chain from the President down to the junior person supporting the mission. Horizontal unity of effort is how different organizations integrate and cooperate with each other even though they have different missions and cultures but have a common purpose and unity of effort.

---

[35] Loren Mooney, "Gen. Stanley McChrystal: Adapt to Win in the 21st Century," Stanford Graduate School of Business, April 15, 2014, accessed November 2, 2017, https://www.gsb.stanford.edu/insights/gen-stanley-mcchrystal-adapt-win-21st-century.

[36] Ibid.

[37] Hooker and Collins, *Lessons Encountered: Learning from the Long War*, 247-248.

Cognition for Decision-Makers: Data Integration and Data Analytics for Soft and Hard Power Options

The contest over information accelerates these political, economic, and military competitions. Data, like energy, will shape US economic prosperity and our future strategic position in the world. The ability to harness the power of data is fundamental to the continuing growth of the US economy, prevailing against hostile ideologies, and building and deploying the most effective military in the world.[38]

The United States and its national interests will continue to experience challenges from Gray Zone adversaries using combinations of non-attributional incrementalism to influence local populations and to create narratives that support their goal of challenging international law or treaties without the cost of economic sanctions or armed conflict. Social media, encrypted messaging applications, misinformation campaigns, and a plethora of other technology and communication platforms enable adversaries to operate anonymously while obfuscating the intent of their operations.[39] For targets of Gray Zone operations, these communication mediums are challenging to monitor and may render friendly narratives or strategic messaging ineffective. Gray Zone actors have access to a wide array of options to shape, control and influence local populations, promote their narratives, and to counter US diplomatic and economic policies while remaining secure in the knowledge that the combination of anonymity and the process to assign attribution takes time.[40] A system or process that can integrate and provide an aggregated picture of information across DoD and the Interagency is an essential part of enabling Gray Zone cognition to support decision-makers developing response options for the National Security Council and the President.

---

[38] Trump, "National Security Strategy of the United States of America," 3.

[39] Cori E. Dauber, "The TRUTH is out there: Responding to Insurgent Disinformation and Deception Operations." *Military Review* (2009): 13-23.

[40] Ibid.

The role of "information warfare" in Gray Zone conflict is indisputable, as states seek to influence both external and internal audiences with messages that legitimate belligerent policy. US defense planners regularly incorporate "information" as an element of national power in their planning processes, and the entire spectrum of political actors in most nations now deploy sophisticated strategies to shape narratives in government communications, popular media, and social media.[41] Information Operations doctrine defines the cognitive domain as the component of the information environment (IE) that encompasses the gray matter of those who transmit, receive, and act upon information.[42] Cognitive operations such as information processing, perception, judgment, and decision- making are the most vital aspect of the IE. Individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies all influence cognition. Thus it requires research and analysis methods from the bio-psycho-social sciences to understand and manipulate.[43]

The Reuter's Institute of News Digital News Report (April 2016) pointed to social media's emergence as a powerful force in global news among twenty-six Asian and Western nations. It has become the primary news source among young people, replacing television, newspapers, and other Web-based platforms.[44] The report argued that algorithms aiming to create "echo chambers" determine the coverage of news on social media. People only see news from

[41] Robert Hinck, Randolph Kluver, and Skye Cooley, "Media Visions of the Gray Zone: Contrasting Geopolitical Narratives in Russian and Chinese Media." Research Project funded through DHS in Support of Strategic Multilayer Assessment (DoD), (College Station, TX, 2017), 1.

[42] Spitaletta, Jason. White Paper on Bio-Psycho-Social Applications to Cognitive Engagement, *Public Intelligence.net.* October 2016, accessed December 22, 2017, https://info.publicintelligence.net/SMA-CognitiveEngagement.pdf.

[43] Patricia DeGennaro, *White Paper on Bio-Psycho-Social Applications to Cognitive Engagement* (Boston: National Security Innovations, 2016), 5.

[44] Ibid.

similar viewpoints with like-minded responses, leading to a fragmented, incomplete, and biased understanding of current issues.[45]

> The notion that a population can be informed, linked together, and systematically divided by algorithmic applications to create echo chambers while disturbing in its own right, offers insight into the power and importance of narrative crafting, narrative management, and information exposure in a globalized media context. 'In essence, each citizen becomes both a target and a weapon for information, and disinformation, in a globalized media context. Controlling narrative exposure within that space has become its own type of Gray Zone conflict. Geopolitical narratives are important because they help to define the political and geopolitical worldview of a population.'[46]

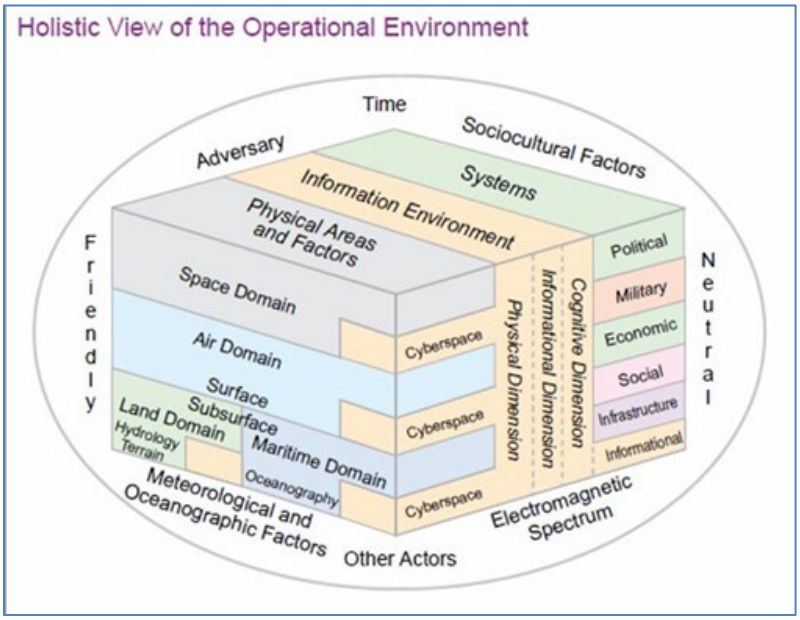

Figure 5. The Operational Environment. Joint Chiefs of Staff, Joint Publication 3-0, *Joint Operations* (Washington, DC: Government Printing Office, January 2017), 5.

An aggregated, actionable, verifiable, and coordinated picture to understand a Gray Zone operation does not exist. This further complicates the cognitive disconnect the US understanding of their adversaries who seek to advance their interests under the auspices of a Gray Zone

[45] Patricia DeGennaro, *White Paper on Bio-Psycho-Social Applications to Cognitive Engagement* (Boston: National Security Innovations, 2016), 5.

[46] Ibid., 6

strategy.[47] Information is an especially important sphere for Gray Zone operations for several reasons. As described earlier, Gray Zone operations are enduring, so there is ample time to see their effects. Many near- and long-term results are overt, rather than covert, although deception and denial are often in play.

Gray Zone operations most often target a population and key individuals who influence others. Many times, overt Gray Zone operations are discoverable through specific analysis techniques.[48] Also, the information battlespace is critical to the United States as it looks to counter Gray Zone operations of competitors and potential adversaries. Technology has enabled a new landscape of influence operations, persuasion, and more generally, mass manipulation. Narratives and influence are also far more concealable where the Internet and social media provide new ways of constructing realities for actors, audiences, and media.[49]

> A particularly instructive incident took place during Operation Valhalla in Iraq in March 2006. A battalion of United States Special Forces Soldiers engaged a Jaish al-Mahdi death squad, killing 16, capturing 17, destroying a weapons cache, and rescuing a badly beaten hostage. In the time it took for the soldiers to get back to their base-less than one hour-Jaish al-Mahdi soldiers had returned to the scene and rearranged the bodies of their fallen comrades to make it look as if they had been murdered while in the middle of prayer. They then put out pictures and press releases in Arabic and English showing the alleged atrocity.
>
> The United States unit had filmed its entire action and could prove this is not what happened. It took almost three days before the United States military attempted to tell its side of the story in the media. The Army was forced to launch an investigation that lasted 30 days, during which time the battalion was out of commission.[50]

The Jaish al-Mahdi operation is an excellent example of how social media and the Internet can inflict a defeat without using physical force. This incident was one of the first clear

---

[47] Defense Science Board. *Summer Study on Capabilities for Constrained Military Operations,* Washington, DC: Office of the Secretary of Defense, 2016. Page 15

[48] RAND Corporation, *The Weaponization of Information*. Page 2-3

[49] Ibid.

[50] Cori E. Dauber, "The TRUTH Is Out There: Responding to Insurgent Disinformation and Deception Operations," *Military Review* (2009): 13-23.

demonstrations of how adversaries can now openly monitor American audience reactions to their messaging in real time, from thousands of miles away and fine tune their actions accordingly.[51]

Information remains an important instrument of national power and a strategic resource critical to national security. Every DoD action, planned or executed, a word that is written or spoken, an image that is displayed or relayed, communicates the intent of DoD, and by extension the USG, with the resulting potential for strategic effects.[52] DoD makes every effort to synchronize, align, and coordinate communication activities to facilitate an understanding of how key audiences will receive or understand the planning and execution of DoD strategies, plans, operations, and activities.[53] Commander's communication guidance is a fundamental component of national strategic direction and is essential in achieving unity of effort through unified action with our Interagency partners and the broader inter-organizational community. An effective combination of themes, messages, images, and actions, consistent with higher-level guidance, is essential to effective DOD operations.[54]

DoD and Interagency Roles for Improving Cognition in the Gray Zone

Understanding Gray Zone environments requires more time and effort to develop a complete picture in an atmosphere where an adversary may be adept at controlling the information environment and the narrative. Using social media to understand deeper constructs of social fragmentation may inform planning recommendations for a wide range of response options

[51] Cori E. Dauber, "The TRUTH Is Out There: Responding to Insurgent Disinformation and Deception Operations," *Military Review* (2009): 13.

[52] The Lightning Press, "Understanding the Instruments of National Power," accessed January 8, 2018, https://www.thelightningpress.com/understanding-instruments-national-power/.

[53] US Air Force, "ANNEX 3-61 Public Affairs Operations," Curtis E. Lemay Center for Doctrine Development and Education, July 28, 2017, accessed December 14, 2017, http://www.doctrine.af.mil/Portals/61/documents/Annex_3-61/3-61-D09-PA-Comm-Synch.pdf?ver=2017-09-19-161454-787.

[54] US Joint Staff, JP 1-0, *Doctrine for the Armed Forces* 2017, I-13.

and what options may be most efficacious. In the recently released unclassified summary of the United States *National Defense Strategy*, Secretary of Defense James Mattis spoke of the danger posed by competitors and adversaries across every domain where the United States has typically had superiority. Secretary Mattis used examples of cyberwarfare and Gray Zone operations "short of open warfare to achieve their ends [including] information warfare, ambiguous or denied proxy operations, and subversion."[55]

Joint Publication 1-0 states that, "the nature of the challenges to the United States and its interests [including Gray Zone conflicts] demand that the Armed Forces operate as a closely integrated joint team with Interagency and multinational partners [where] unity of effort is achieved through close, continuous Interagency and interdepartmental coordination and cooperation to overcome discord, inadequate structure and procedures, incompatible communications, cultural differences, and bureaucratic and personnel limitations."[56]

Even more challenging for the DoD is the fact that it does not use many of the tools needed to engage in the Gray Zone.[57] The types of information necessary in understanding and influencing an adversary's Gray Zone campaigns are also distinct from traditional collections that focus on an adversary's military power. Not only do Gray Zone campaigns need distinct types of information from traditional combat operations, but relevant sources of information are also different.[58] The US standard intelligence apparatus focuses on the traditional intelligence sources (INTs), including human intelligence, imagery intelligence, and signals intelligence, where

---

[55] US Secretary of Defense, *2018 National Defense Strategy*, 3.

[56] Ibid., xv.

[57] Defense Science Board, *Summer Study on Capabilities for Constrained Military Operations* (Washington, DC: Office of the Secretary of Defense, 2016), Page 31.

[58] Patricia DeGennaro. The Gray Zone and Intelligence Preparation of the Battle Space, *Small Wars Journal.* August 17, 2016, accessed October 22, 2017. http://smallwarsjournal.com/jrnl/art/the-gray-zone-and-intelligence-preparation-of-the-battle-space.

specialized assets are acquired and then tasked for specific, targeted collection. These INTs are highly relevant to Gray Zone campaigns in thwarting the US adversaries' goals, and in designing and prosecuting proactive campaigns.[59]

Countering Gray Zone competitors successfully requires intelligence information not only from the Intelligence Community but from the Interagency and non-governmental sources (business, non-governmental organizations, academic, and others) with contacts, skills, experience, and socio-cultural understanding relevant to the problem, identifying critical vulnerabilities in crucial countries at risk. Energy, natural resources, cyber, financial systems, and governance integrity should be a high priority for US intelligence.[60]

Technology has changed the geopolitical landscape of global competition. The advent of artificial intelligence-enabled big data analytics changes the relationship of man to machine. This can alter risk management strategies for Gray Zone actors allowing them to vie for political advantage without resorting to traditional warfare. In future warfare, the distinction between combatants and non-combatants, as the DoD traditionally defines them, will be more challenging to make in this strategic environment. The 2018 *NDS* recognizes the reality of how disruptive the rapid advancement and availability of technology has on the global security environment.[61] Technology enables a wider range of actors to take part and complicates how the United States perceives competition and threats from state and non-state actors who target American interests. Secondly, the *NDS* recognizes the United States is in a long-term strategic competition with China and Russia, both expert practitioners of Gray Zone strategies who use "corruption,

[59] United States Army Special Operations Command, *Perceiving Gray Zone Indications.* White Paper, Fort Bragg, NC: U.S. Army Special Operations Command, last revised March 15, 2016, accessed January 2, 2018, http://www.soc.mil/Files/PerceivingGrayZoneIndicationsWP.pdf, 8-15.

[60] ISAB, *Gray Zone Conflicts*, 10.

[61] Ibid., 3.

predatory economic practices, propaganda, political subversion, proxies, and the threat or use of military force to change facts on the ground."[62]

Responding to Gray Zone strategies requires focus and resources to ensure the Untied States is postured to respond across the conflict spectrum to meet and defeat peer and non-state actors alike who threaten American interests. Building and enabling the Interagency to understand and respond to challenges to American influence and interests is essential for success. The *NDS* captures the importance of an integrated Interagency where, "strategic competition requires the seamless integration of multiple elements of national power-diplomacy, information, economics, finance, intelligence, law enforcement, and military–[to leverage] competitive advantages, [build] strong alliances and partnerships, and leveraging American technological innovation."[63]

It is essential in Gray Zone conflicts to understand the overall population and dynamics of each involved nation, including adversary populations and friendly-nation populations targeted by an adversary. An analysis of the general population and society includes an overall understanding of cultural values, interests, biases, and how these general belief systems play out within society. The primary point is that throughout history, the United States has not constructed civilian and military teams for cognitive engagement, its national security structure and system is not organized to encourage a more holistic process needed to address cognitive engagement. The US effort needs teams of people, civilian and military, to cooperate on planning, implementing and assessing outcomes.[64]

The types of information necessary in Gray Zone campaigns are different from those needed for combat operations and include whether to understand an adversary's campaign or to conduct a proactive United States campaign. The DoS Global Engagement Center could be an

[62] Ibid.

[63] ISAB, *Gray Zone Conflicts*, 4.

[64] Ibid., 17.

important part of creating intelligence and valuable expertise. The FY 2017 NDAA expanded the GEC's mission to include countering the adverse effects of state-sponsored propaganda and disinformation. The 2017 NDAA also provided legal authorities, including a Privacy Act authorization, which permits the GEC to meet the rising demand from the Interagency and international partners for data analytics. It charged the GEC's Science and Technology team with enabling the USG and its partners to increase the reach and effectiveness of their communications. The team conducts research on target audiences and utilizes data science techniques to measure the effectiveness of its efforts. Among other techniques, the Science and Technology team performs A/B testing and multivariate analysis to measure the effectiveness of [friendly] content distribution. The GEC's staff includes detailees from throughout the Interagency , including the Department of Defense, Intelligence Community, United States Agency for International Development, and Broadcasting Board of Governors. One of the GEC's overarching strategies is to identify, cultivate, and expand a global network of partners whose voices resonate with individuals most vulnerable to harmful propaganda. Lastly, the GEC and its partners have established programming across multiple platforms, including social media, satellite television, radio, film, and print conducted in various languages. These platforms allow the USG and its partners to inject factual content about terrorist organizations into the information space to counter recruitment and radicalization to violence.[65]

Conclusion

Secretary Mattis recently said that "to succeed in the emerging security environment, our Department and Joint Force will have to out-think, out-maneuver, out-partner, and out-innovate revisionist powers, rogue regimes, terrorists, and other threat actors."[66] The consequences are a

[65] US Department of State, "Under Secretary for Public Diplomacy and Policy Affairs: Global Engagement Center (GEC)," accessed December 20, 2017, https://www.state.gov/r/gec/.

[66] Ibid.

failure to integrate and synchronize operations between DoD, the Interagency and national decision-makers sub-optimizes how the United States understands, deters, and responds to Gray Zone threats and may potentially erode American prestige and allied confidence. DoD and its Interagency partners must be able to work together in a focused, collaborative way with unity of effort in order to be effective. New sources of information derived from social media, the IoT, and advanced data analysis methods integrated with conventional intelligence is essential to prevent, deter, and counter Gray Zone competition. The United States is rapidly developing data analysis tools within the government and commercial sector which they need to apply to the preparation and execution of campaigns.

Cognitive improvements that rely on DoD, Interagency, and non-traditional sources of information will be essential to understanding how a Gray Zone actor works across multiple domains in a comprehensive way so that an aggregated picture of the operational environment is possible. The lack of a comprehensive and integrated picture in a Gray Zone operating environment unnecessarily limits cognition, potentially wastes resources, and may sub-optimize response options.

The Gray Zone is a challenging place for the DoD since the United States tends to treat each incursion as a discrete event and then asks if that event is a threat to American strategic national interests. US competitors and potential adversaries are calculating that the United States will not be willing to make a significant response to their actions. Even more so, these competitors are designing their actions to ensure that the United States will not respond in a significant way. DoD and the Interagency need to collaborate and cooperate to organize and build capacity to show Gray Zone actors they have misjudged American power.

Bibliography

Bertram, Ian. "We Need Effective Operations in the Realm of Social Media: The United States Military and Government Must Effectively Harness the Power of Social Media." *Foreign Policy.* April 21, 2016. Accessed September 6, 2017. http://foreignpolicy.com/2016/04 /21 /essay-contest -13-we-need-effective-operations-in-the-realm-of-social-media/.

Bartles, Charles K. "Getting Gerasimov Right." Military Review 96, no. 1 (January/February 2016): 30-38.

Bragg, Belinda. *Gray Zone Conflicts, Challenges, and Opportunities: Integration Report.* Arlington, VA: National Security Innovations, 2017.

Brands, Hal. "Paradoxes of the Gray Zone." *Foreign Policy Research Institute.* February 5, 2016. Accessed August 16, 2017. https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

Brundick, Frederick S., and Josh Dehlinger. "IChart: A Tool For Visualizing and Managing Organizational and Force Structure Data." Presentation, 16th International Command and Control Research and Technology Symposium, Quebec, Canada, June 21-23, 2011. Accessed February 11, 2018. http://dtic.mil/cgi-bin/gettrdoc?ad=ada547388& location=u2&doc=gettrdoc.pdf.

Chairman, Joint Chiefs of Staff. CJCSI 3100.01C, *Joint Strategic Planning System (JSPS).* Washington, DC: Government Printing Office, 2015.

———. Joint Publication 1-0, *Doctrine for the Armed Forces.* Washington, DC: Government Printing Office, 2017.

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

———. Joint Publication 5-0, *Joint Planning.* Washington, DC: Government Printing Office, 2017.

Clark, Colin. "CJCS Dunford Calls for Strategic Shifts: 'At Peace or At War is Insufficient'." *Breaking Defense*. September 21, 2016. Accessed October 17, 2017. https//breakingdefense.com/2016/09/cjcs-dunford-calls-for-strategic-shifts-at-peace-or-at-war-is-insiffiecient/.

Dauber, Cori E. "The TRUTH Is Out There: Responding to Insurgent Disinformation and Deception Operations." *Military Review* (2009): 13-23.

Defense Science Board. *Summer Study on Capabilities for Constrained Military Operations.* Washington, DC: Office of the Secretary of Defense, 2016.

DeGennaro, Patricia. *White Paper on Bio-Psycho-Social Applications to Cognitive Engagement.* Boston: National Security Innovations, 2016.

———.The Gray Zone and Intelligence Preparation of the Battle Space, *Small Wars Journal.* August 17, 2016. Accessed October 22, 2017. http://smallwarsjournal.com/jrnl/art/the-gray-zone-and-intelligence-preparation-of-the-battle-space.

Elkus, Adam. “50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense.” *War on the Rocks*. Last revised December 15, 2015. Accessed September 29, 2017. https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense.

Feickert, Andrew. 2013. "The Unified Command Plan and Combatant Commands: Background and Issues for Congress." *Congressional Research Service.* January 3. Accessed October 9, 2017. https://fas.org/sgp/crs/natsec/R42077.pdf.

Freedberg, Sydney J. “Joint Staff Must Boost Global Coordination; No New Powers Needed: J5.” *Breaking Defense.* April 27, 2017. Accessed November 30, 2017. https://breakingdefense.com/2017/04/joint-staff-must-step-up-global-coordination-no-new-powers-needed-j-5/.

Hinck, Robert, Randolph Kluver, and Skye Cooley. “Media Visions of the Gray Zone: Contrasting Geopolitical Narratives in Russian and Chinese Media.” Research Project funded through DHS in Support of Strategic Multilayer Assessment (DoD), College Station, TX, 2017.

Hooker, Richard D., and Joeseph J. Collins. *Lessons Encountered: Learning from the Long War.* Washington, DC: National Defense University Press, 2015.

International Security Advisorry Board (ISAB). *Gray Zone Conflicts.* Washington, DC: United States Department of State, 2017.

Mazarr, Michael J. 2015. "Mastering the Gray Zone: Understand a Changing Era of Conflict." *United States Army War College Strategic Studies Institute.* December. Accessed November 12, 2017. https://ssi.armywarcollege.edu/pdffiles/PUB1303.pdf.

Matisek, Jahara, and Ian Bertram. “The Death Of American Conventional Warfare: It’s The Political Willpower, Stupid.” *The Strategy Bridge.* November 5, 2017. Accessed December 1, 2017. https://thestrategybridge.org/the-bridge/2017/11/5/the-death-of-american-conventional-warfare-its-the-political-willpower-stupid.

McChrystal Group. “Team of Teams.” Accessed January 6, 2018. https://www.mcchrystalgroup.com/insights/teamofteams/.

McInnis, Kathleen J. *Goldwater-Nichols at 30: Defense Reform and Issues for Congress.* Washington, DC: Congressional Research Service, 2016.

Mooney, Loren. “Gen. Stanley McChrystal: Adapt to Win in the 21st Century.” Stanford Graduate School of Business. April 15, 2014. Accessed November 2, 2017. https://www.gsb.stanford.edu/insights/gen-stanley-mcchrystal-adapt-win-21st-century.

National Archives and Records Administration. “Agency Filter.” *Federal Register.* January 15, 2018. Accessed January 15, 2018. https://www.federalregister.gov/agencies.

National Intelligence Council. “Foreign Approaches to Gray Zone Conflicts.” Accessed September 25, 2017. http://nsiteam.com/foreign-approaches-to-gray-zone-conflicts/.

Pomerantsev, Peter. “Inside the Kremlin's Hall of Mirrors.” *The Guardian.* April 9, 2015. Accessed September 25, 2017. https://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology.

RAND Corporation. *The Weaponization of Information: The Need for Cognitive Security.* Testimony of Rand Waltman Before the Committee on Armed Services Subcommittee on Cybersecurity United States Senate. Santa Monica, CA: RAND Corporation, 2017.

Scharre, Paul. “American Strategy and the Six Phase of Grief.” *War on the Rocks.* October 6, 2016. Accessed December 9, 2017. https://warontherocks.com/2016/10/american-strategy-and-the-six-phases-of-grief/.

Spitaletta, Jason.. "White Paper on Bio-Psycho-Social Applications to Cognitive Engagement." *Public Intelligence.net.* October 2016. Accessed December 22, 2017. https://info.publicintelligence.net/SMA-CognitiveEngagement.pdf.

The Lightning Press. “Understanding the Instruments of National Power.” Accessed January 8, 2018. https://www.thelightningpress.com/understanding-instruments-national-power/.

Trump, Donald J. “National Security Strategy of the United States of America.” Whitehouse.gov. December 2017. Accessed January 2, 2018. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

US Air Force. “ANNEX 3-61 Public Affairs Operations.” Curtis E. Lemay Center for Doctrine Development and Education. July 28, 2017. Accessed December 14, 2017. http://www.doctrine.af.mil/Portals/61/documents/Annex_3-61/3-61-D09-PA-Comm-Synch.pdf?ver=2017-09-19-161454-787.

US Department of Defense. “Remarks on “Goldwater-Nichols at 30: An Agenda for Updating.” April 5, 2016. Accessed January 4, 2018. https://www.defense.gov/News/Speeches/Speech-View/Article/713736/remarks-on-goldwater-nichols-at-30-an-agenda-for-updating-center-forstrategic/.

US Army Special Operations Command. *Perceiving Gray Zone Indications*, Fort Bragg, NC: U.S. Amry Special Operations Command, March, 15, 2016, Accessed January 2, 2018, http://www.soc.mil/Files/PerceivingGrayZoneIndicationsWP.pdf.

US Department of State. “Under Secretary for Public Diplomacy and Policy Affairs: Global Engagement Center (GEC).” Accessed December 20, 2017. https://www.state.gov/r/gec/.

US Secretary of Defense. *Summary of the 2018 National Defense Strategy of the United States of America.* Washington, DC: US Department of Defense, 2018.

Votel, Joseph L, Charles T. Cleveland, Charles T. Connett, and Will Irwin. “Unconventional Warfare in the Gray Zone.” *Joint Force Quarterly* 80, no. 1 (2016): 101-109.

Whitehouse.gov. “National Security Council.” December 1, 2017. Accessed December 12, 2017. https://www.whitehouse.gov/nsc/.

Wright, Nicholas D. *From Control to Influence: Cognition in the Grey Zone.* Report for the Pentagon Joint Staff Strategic Multilayer Assessment Group, Birmingham, UK: Institute for Conflict, Cooperation and Security, University of Birmingham, UK. 2017.