The Report Committee for Travis Wayne Miller
Certifies that this is the approved version of the following Report:

Organizing for Hybrid and Information Warfare

APPROVED BY
SUPERVISING COMMITTEE:

William Inboden, Supervisor

Stephen Courter

Organizing for Hybrid and Information Warfare

by

Travis Wayne Miller

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degrees of

Master of Global Policy Studies

and Master of Business Administration

The University of Texas at Austin

May 2020

Acknowledgements

This professional report was an intellectually stimulating journey, but it was only accomplished through the guidance, constructive feedback, and support from so many. Professor William Inboden's patience and direction allowed me to explore and reflect throughout this process—his sage advice will accompany me throughout my professional career. Stephen Courter's instruction on organizational management guided me through the process of cutting the red tape. Professor Kiril Avramov spurred my intellectual curiosity and provoked great dialogue throughout this research. I would like to also acknowledge Professor John Doggett, who has provided me with resources and opportunities, and challenged my critical thinking throughout my time in graduate school. Writing is not my forte, but this paper would not be in the shape it is in today without the constructive feedback from my writing coach and professors at the Lyndon B. Johnson School of Public Affairs. I would be remiss if I did not recognize my wife and sons who were patient and understanding during many coffee shop dates with my computer and books, and the early mornings and late nights on campus. Thank you all for the support on this intellectual journey.

I am an active-duty service member and was privileged to have talked to many people throughout this study. The thoughts and opinions in this report are mine and do not reflect the position of the United States Government, Department of Defense, or the graduate programs I attended at the University of Texas at Austin. I do not have access to current government documents nor other related government efforts regarding hybrid or information warfare strategies, in which my professional report might misrepresent ongoing efforts.

Abstract

Organizing for Hybrid and Information Warfare

Travis Wayne Miller, MGPS & MBA
The University of Texas at Austin, 2020

Supervisor: William Inboden

This professional report argues that current national security documents and the national security structure are not optimized to conduct hybrid and information warfare. It reviews an abundance of literature to first understand the United States national security strategy, coupled with the reemergence of great power competition. Four propositions emerged from the readings: national security publications are incoherent; a strategic paralysis has set in with the abundance of literature; there is a lack of organizational innovation; and the instruments of national power have tilted towards information. Following this review, the analysis then explores Russia's great power competition strategy through private/public, legal/illegal, and regular/irregular lenses. China's information warfare strategy, *Three Warfares*, which includes propaganda, public opinion, and legal warfare, provides the final piece of analysis on great power competition. This conflict is particularly vast—the hybrid approach calls on all elements of a nation's society; information is the dominant power shaping perceptions, decisions, opinions, and behaviors; and all this is conducted in the gray zone between peace and total war. The report then investigates the most recent declassified information warfare campaign against a great power, Operation QRHELPFUL, and a recent example of information leveraged as the main effort in a combined joint military operation. The United States can organize more effectively for the challenges it confronts by understanding the principles, lessons learned, and the context of great power competition. This requires vertical and horizontal organizational efforts, which include a shift in policy, a new organizational framework, assigning a lead, and adopting a whole-of-society approach.

Table of Contents

List of Tables vii

List of Figures viii

Introduction 1

Literature Review 5

Hybrid and Information Warfare Defined 7

Proposition 1: National security publications are incoherent 9

Proposition 2: The abundance of literature creates strategic paralysis 11

Proposition 3: Ineffective organizational structure for great power competition 11

Proposition 4: The instruments of national power tilt towards information warfare 13

Great Power Analysis 15

Russia's Renewed Military Thinking 15

The Rise of Sun Tzu in China 21

Historical and Recent U.S. Information Warfare Examples 28

Operation QRHELPFUL 28

Information as the Main Effort 31

Implications 39

Recommendations 43

1. Create a policy of ambiguity and establish a working group 43

2. Formalize a Joint Interagency Task Force 45

3. An organization to initially lead the effort—SOF 47

4. Enhance Public-Private cooperation and collaboration 48

Conclusion 50

References 52

List of Tables

Table 1: Segments of Base/Enabler Methodology.....34

Table 2: Segment characteristics 34

List of Figures

Figure 1: Psychographic profile of the Base/Enabler Methodolgoy 33

Figure 2: Opinions on Yemen's governmental structure vary.....36

Introduction

Thirty years after the peaceful end of the Cold War, the United States is now entering a new era of great power competition. Emerging and resurgent great powers, Russia and China, stand as the primary national security threats to the United States, as defined in the 2017 National Security Strategy (NSS). The 2018 National Defense Strategy (NDS), nested within the 2017 *NSS*, identified "inter-state strategic competition, not terrorism, as the primary concern for United States national security."[1] These threats from great powers are multi-domain; they exist across all elements of national power: diplomatic, information, military, and economic. The 2018 *NDS* identifies revisionist powers and rogue regimes competing across the full spectrum of domains and capabilities: "they [great powers] have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals."[2] In particular, threats in the information environment have created a considerable strategic, operational, and tactical challenge for the United States to counter.[3] This leaves the current international order ripe for disruption.

Yet, despite these official acknowledgements of the threats facing the United States, the nation has done little to implement a strategy that would combat these threats, to orient its institutions towards blunting them, or to mobilizing the parts of society that are needed if the United States is to confront these challenges. As this work will argue, the reason for this lack of follow-through has do with the incoherence of strategic documents, the sheer number of conflicting analyses, and the lack of proper organization.

---

[1] *2018 National Defense Strategy Summary*, (The Department of Defense, 2018). Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, 1.
[2] Ibid, 2.
[3] *2017 National Security Strategy of the United States of America*, (The White House, December 2017). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Since the dawn of the Information Age in the 1970s, the use of information as an instrument of national power has become more influential and effective in accomplishing national strategic objectives, as well as posing new dimensions of threats to the United States from its adversaries. In the words of the *NSS*, "America's competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information."[4] Weaker nation-states and non-state actors, to a considerable degree, are also enabled by the democratization and distribution of information technologies. These technologies advance and are exploited at a speed and scale far greater today than at any time in history. Because of this, as Rory Cormac and Richard Aldrich argue, "Russia believes that a single global 'information space' is emerging, which could allow a country to exploit this space and alter the global balance of power."[5] Russia, for example, following the collapse of the Berlin Wall has utilized advances in information technology to exploit vulnerabilities of the United States throughout the information environment, impacting both domestic and foreign interests. China's information warfare strategy, known as *Three Warfares*, is a direct challenge to the United States' global influence and directly shaping the geopolitical landscape. [6]

These threats are acknowledged at the highest level, but little has been done to adapt and counter them. The 2017 *NSS* acknowledges that "U.S. efforts to counter the exploitation of information by rivals has been tepid and fragmented."[7] In particular, there has been little organizational change to maintain the United States' competitive advantage within the current

---

[4] Ibid, 34.

[5] Cormac, Rory and Richard Aldrich. *Grey is the New Black: Covert Action and Implausible Deniability*, (International Affairs, May 2018). Retrieved from https://academic.oup.com/ia/article/94/3/477/4992414, 66.

[6] China's Three Warfares, or information warfare, strategy includes three core concepts: public opinion warfare, psychological warfare and legal warfare.

[7] *2017 National Security Strategy of the United States of America*, 34.

international order. The Department of Defense (DoD) objectives in the *NDS* prioritized Russia and China as long-term strategic competition; however, in outlining the eleven stated objectives, none of them focused on hybrid or information warfare strategies. As Sean McFate articulated in a recent article for *Medium Corporation*: "In the future, victory will be won and lost in the information space, not on the physical battlefield. It's absurd that the West has lost information superiority in modern war, given the heaps of talent in Hollywood, on Madison Avenue, and in London. The West's squeamishness about using strategic subversion only helps its enemies."[8] To understand these threats and challenges, which seamlessly cross national borders, dominate geography, and impact the full spectrum of society, the response must start with organizing.

The United States needs a new strategy and to operationalize information warfare to maintain its competitive advantage in the 21st-century. Instead of a whole-of-government approach, the United States must mobilize a whole-of-society effort and incorporate it at the operational and tactical levels, not just at the strategic level within the National Security Council. To counter closed-states and organizations, greater integration and collaboration across the government and private sector are required. In addition to decentralized operational authority to wield the national instruments of power at a scale and speed equal to United States adversaries. Furthermore, Special Operation Forces (SOF) are a unique element strategically positioned to carry out hybrid and information warfare campaigns. The United States must challenge traditional military thinking and operational frameworks and shift its attention to influence and shape the narrative. SOF can be a means to utilize against great powers and influence the narrative in support of United States national security objectives. The fundamental tenet to conduct information

[8] McFate, *The Return of Mercenaries*.

warfare is through a decentralized “whole-of-society” approach, in which US SOF is currently positioned to lead.

The following sections will define hybrid warfare, information warfare and gray zone conflicts; highlight four propositions based on the literature review; and analyze Russia’s and China’s hybrid and information warfare strategies. These sections will frame the complex strategic environment that provides context for studying two cases where the United States has taken an active role in shaping the information environment. Lastly, the implications of this analysis, along with recommendations for an organizational design, will provide a framework that the United States can operationalize against great power competition.

Literature Review

The research examined here focuses on the resurgence of great powers and their use of information to challenge the current international order through a whole-of-society approach. The principles and lessons learned that underline the use of information as a strategy, known as information warfare, were primarily identified through qualitative research coupled with empirical evidence through interviews and the use of collected data. It will review and provide a synopsis of great power hybrid and information warfare strategies, like Russia's employment of General Gerasimov's hybrid warfare strategy—often referred to as the *Gerasimov Doctrine*.[9] It will identify specific examples of Russia's use of Spetsnaz forces, and how other entities of their society use subversive means to achieve Russian national strategic objectives. China's *Three Warfares* was analyzed through open-source publications and other research articles and journals. This research is an aggregate of numerous articles, journals, official government documents, historical case studies, expert interviews, polling, and analysis, through the lens of personal experience.

To understand the nuances of conflict in the 21st-century, several professors with expertise on Russia and hybrid warfare, former Central Intelligence Agency officers, and former members of the National Security Council were consulted. Interviews with retired senior military officers and three General Officers were conducted as well. These interviews included General Vincent Brooks, former Commanding General United States Forces Korea, United Nations Command, and Republic of Korea-U.S. Combined Forces Command; Major General Ed Reeder, former Commanding General, Special Operations Joint Task Force-Afghanistan / NATO Special Operations Component Command-Afghanistan; and Lieutenant General Jeffrey Buchanan, former

[9] The name "Gerasimov Doctrine" was given by scholars when General Gerasimov first published a thought piece on non-linear / hybrid warfare, but it should not be confused as actual Russian doctrine.

Commander, U.S. Army North (Fifth Army). These conversations focused on the strategic implications of hybrid and information warfare, examples of United States efforts in great power competition, and how the United States national security structure can organize to optimize a hybrid and information warfare strategy. In many ways, the challenges the United States faces are inherently a struggle between being effective and of upholding values. The baseline for any United States approach must first and foremost not compromise United States' values—across all interviews, this was critical to the foundation of formulating a strategy for great power competition.

The recently published book by Seth Jones, *A Covert Action: Reagan, the CIA, and the Cold War Struggle in Poland* was the primary source for the most recent unclassified information warfare operation against a great power. Jones provides a comprehensive review of Operation QRHELPFUL and several key factors associated with this Central Intelligence Agency (CIA) led covert action program.[10] His analysis of the strategic situation, the complex challenges, and the program design correlates similarly to what the United States faces today involving great powers.

In the analysis of a recent United States information warfare example, polling data was used to shape the strategy. The data, about security issues in Yemen, came from a March 2017 Yemen Polling Center for the European Union and a U.S. Central Command (CENTCOM) commissioned survey from May-August 2018. Both sets of data are thorough and consistent with traditional polling practices. The data collected is also unclassified; however, due to the nature of the collection and governing authority over the data it is not releasable at this time. Some of the data was selected to present an objective viewpoint, and to illustrate how an information warfare

[10] Many of the original classified documents and historical information regarding Operation QRHELPFUL reside in the National Archives, presidential libraries or were retrieved through personal interviews that were unattainable due to logistical constraints.

strategy shaped the environment and conditioned behaviors prior to the operation. Before moving further, it is important to get on the same page with defining a few key terms. Though the definitions of the following terms vary, by defining them here, it helps frame the understanding and argument in this paper.

Hybrid and information warfare defined

Hybrid warfare, information warfare, and gray zone conflict are not new terms. However, there are multiple articles and research journals that utilize these terms in abundance—drawing attention by describing the reemergence of great power competition and rising conflicts short of conventional war. These terms are extensively used throughout this paper and draw on key definitions and thoughts from subject matter experts.

Hybrid warfare has been a Western military term for decades. It was also not foreign to James Mattis—an American Lieutenant General at the time and later President Trump's Secretary of Defense—who wrote about it in when it appeared in a 2005 title he authored.[11] For this research paper, hybrid warfare is defined based on an article in the Combating Terrorism Exchange (CTX) Special Issue on Countering Hybrid Warfare. In CTX, Frank Steder, at the Norwegian Defense Research Establishment, writes an article on the theory and history of hybrid warfare. He defines hybrid warfare as the "use [of] all means necessary—conventional and non-conventional, legal and illegal, regular and irregular—to weaken an adversary across time, level and place before war is declared." Furthermore, according to Frank Hoffman, retired Marine Corps Lieutenant Colonel and author of *Conflict in the 21st Century: The Rise of Hybrid Wars*, states hybrid warfare's chief characteristics are convergence and combinations. He describes these characteristics as "various

[11] Kramer, A. *Russian General Pitches 'Information' Operations as a Form of War,* (The New York Times, March 2, 2019). Retrieved from https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.

methods and actions, spanning all sectors of society, are combined and deployed simultaneously to present the opponent with a complex and overwhelming situation."[12] Hoffman highlights how warfare is converging within and combining, not just a whole-of-government but a whole-of-society, to shape the geopolitical arena.

The definition of information warfare remains highly debated. In fact, the United States currently has no official definition. Information warfare is one sub-category of hybrid warfare, albeit a significant one. Some research suggests information warfare is the range of kinetic and non-kinetic operations to protect and exploit the information environment, consisting of both defensive and offensive measures. Conrad Crane, a retired Army officer and historian, is clear and concise in his description of information warfare. Defining it as the "gathering, providing, and denying information in order to improve one's own decision-making while damaging the enemy's."[13] Scott Johnson from the CIA's Center for the Study of Intelligence, shares a similar sentiment as Crane, but provides a more comprehensive description of information warfare in his article, *Toward a Functional Model of Information Warfare*. For this research paper, Johnson definition of information warfare—which focuses on the decision-making aspect of an adversary—will be used:

> "The ultimate target of information warfare is the way in which information is used—that is, the decision process. The desired effects of information warfare attacks may be indirect—not just blinding or confusing the enemy, but shaping his perceptions, decisions, opinions, or behavior. The

[12] Hoffman, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars,* (Potomac Institute for Policy Studies, December 2007). Retrieved from https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, 9.
[13] Crane, Conrad. *The U.S. Needs and Information Warfare Command: A Historical Examination,* (Information Professionals Association, June 14, 2019). Retrieved from https://information-professionals.org/the-u-s-needs-an-information-warfare-command-a-historical-examination/.

> information warfare planner's understanding of the target has to extend to this layer, and knowledge of the adversary has to include his decision criteria, decision processes and time scales, and vulnerabilities."[14]

Where in the spectrum of conflict does this take place? General Joseph Votel, former Commanding General U.S. Central Command, offered valuable insight of gray zone conflicts and characterized them "by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."[15] Thus, when these definitions are coupled together, the reemergence of great power competition can be framed in the space between peace and total war, utilizing a hybrid warfare strategy to incorporate all societal elements of national power, and leveraging the information environment to shape the decisions of the adversary. Understanding the context of great power competition through these definitions is fundamental for the argument imposed in this paper. The following propositions identify strengths and weaknesses of the literature reviewed at large.

Proposition 1: National security publications are incoherent

Research reviewed official government documentation focused on the 2017 *NSS* and respective *Priority Actions* sections to understand how the United States was thinking about the current fight and the overarching strategy to address hybrid and information warfare threats. The 2017 *NSS*, the 2018 *NDS*, as well as the fiscal year 2020 resourcing strategy for the 2018 *NDS*, spoke of the reemergence of great power competition from Russia and China as top national

[14] Johnson, Scott. *Toward a Functional Model of Information Warfare,* (Center for the Study of Intelligence, April 14, 2007). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html.

[15] Votel, Joseph , Charles Cleveland, Charles Connett and Will Irwin. *Unconventional Warfare in the Gray Zone,* Joint Force Quarterly 80, (National Defense University Press, January 2016). Retrieved from https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.

security threats. However, these documents were ineffective capturing the threat from Russia and China's information warfare strategies that are disrupting the current international order and the global influence of the United States.

These strategic documents also failed to address organizational strategies. Therefore, additional research focused on former and current organizations who were and are tasked to execute hybrid and information warfare activities. These included the Central Intelligence Agency, United States Information Agency (USIA), and the DoD. The USIA, however, was disbanded in 1999, and there was a lack of metrics and details associated with how successful they were throughout the Cold War executing information operations (IO). There is a full spectrum of United States military publications on the subject to include: the Joint Publications on Information Operations, the Joint Concept for Human Aspects of Military Operations (JC-HAMO), and numerous other research journals and opinion articles, both foreign and domestic. The JC-HAMO provided the most comprehensive and inclusive design for the art and intent of information warfare—the need to understand relevant actors' motivations and the underpinnings of their will.[16] The concept recognizes that war is fundamentally and primarily a human endeavor, and, thus, captures the necessity of incorporating the human aspect of warfare when shaping the United States national security strategy. However, the JC-HAMO was published in October of 2016, and it appears it has not been fully incorporated into operational planning. With so much information, it is has become overbearing to formulate an effective strategy and organize to execute it.

[16] *Joint Concept for Human Aspects of Military Operations*, (Joint Chiefs of Staff, October 19, 2016). Retrieved from https://nsiteam.com/social/wp-content/uploads/2017/01/20161019-Joint-Concept-for-Human-Aspects-of-Military-Operations-Signed-by-VCJCS.pdf.

Proposition 2: The abundance of literature creates strategic paralysis

There is much to admire about the attempt to understand the resurgence of great power competition. Hybrid warfare, information warfare, political warfare, non-linear warfare, are current buzz words in academia, think tanks, and within the Washington beltway. However, in the last decade and to an increasing scale; national security meetings, think tanks, academic conferences, research journals, and published books on 21st-century warfare have occurred more and more often to the point of strategic decision paralysis. Numerous articles discuss what and how the United States might go about conducting or countering hybrid and information warfare, but little has changed internally to the DoD, Department of State (DoS), or any other governmental agency to operationalize hybrid and information warfare. Few have answered how the United States should organize to conduct or counter adversaries in the segment of the conflict continuum known as the gray zone. Thus, there lacks a comprehensive organizational approach to counter and conduct hybrid and information warfare.

Proposition 3: Ineffective organizational structure for great power competition

The United States has vulnerabilities in its current organizational structure to counter and execute hybrid warfare capabilities. This is illustrated in the insufficient changes in the United States national security organizational structure, a lack of authorities, as well as a lack of appropriate resourcing in the U.S. National Defense Budget. The 2018 *NDS* calls for difficult choices to "field a lethal, resilient and rapidly adapting Joint Force," however reviewing the fiscal year 2020 resourcing strategy for the 2018 *NDS* highlights otherwise.[17]

[17] *2018 National Defense Strategy Summary*, 3.

To understand the reality of priorities, follow the money. The DoD Comptroller, David L. Norquist, testified before Congress on the fiscal year 2020 "strategy-driven budget" in support of the 2018 *NDS*.[18] Though the DoD budget for fiscal year 2020 focused on the development of conventional military capabilities in the traditional realms of conflict, it lacked resourcing support for a hybrid or information warfare capability. Norquist said, "if you want peace, our adversaries need to know there's no path to victory through fighting us."[19] Adversaries of the United States likely do understand this, and it is why they have tilted their strategies towards hybrid warfare and the asymmetric advantages it offers them in the information environment. The United States must address the hybrid aspect in which great powers are contesting its influence across the globe, as well as domestically, as seen in more recent years with the meddling in the 2016 Presidential elections.

There were also numerous academic journals like the *Combating Terrorism Exchange*, *Norway's Special Operations Forces 2025* research paper, and others that provided examples on who, what, and how to counter these threats. However, they relied too heavily on the current military structure, which extends back to Napoleon's era of combined arms, and not enough on how integrated society has become that requires a more effective whole-of-society approach. Even the intelligence community efforts and proactive policy options should call for the needed changes and more appropriate resourcing to ensure the United States remains resilient against great power competition.

---

[18] Vergun, David. *DOD Comptroller: Overmatch Against China, Russia* Critical, (U.S. Department of Defense, April 10, 2019). Retrieved from https://www.defense.gov/Explore/News/Article/Article/1810790/dod-comptroller-overmatch-against-china-russia-critical/.

[19] Ibid.

Proposition 4: The instruments of national power tilt towards information warfare

Great powers have changed their strategies and organizational entities to be more effective in hybrid and information warfare. As the *NSS* states, United States "rivals compete across political, economic, and military arenas, and use technology and information to accelerate these contests in order to shift regional balances of power in their favor."[20] The effective use of diplomacy, military, and economic instruments of national power have been utilized to a far greater scale than information—the latter, however, has become far more influential in recent decades. Traditionally, we see the United States departments who embody these national powers, like the DoD, DoS and Department of Treasury, converge within the interagency process of the National Security Council. However, this whole-of-government approach is wielded only at the strategic level of government, which is cumbersome and slow to counter any threats.

The 2017 *NSS* also describes the United States adversaries adapting and operating "below the threshold of open military conflict and at the edges of international law."[21] United States policy-makers look at the world through a black and white lens, formulate policies and utilizing the instruments of national power to maintain this framework of international order.[22] However, gray is the new black when it comes to shifting the global balance of power. In The New Rules of Warfare, Sean McFate states: "wars will move further into the shadows. In the information age, anonymity is the weapon of choice...Conventional military forces will be replaced by masked ones that offer plausible deniability, and non-kinetic weapons, like deception and influence, will prove decisive. Shadow war is attractive to anyone who wants to wage war without consequences, and

[20] *2017 National Security Strategy of the United States of America*, 25.
[21] *2017 National Security Strategy of the United States of America*, 27.
[22] Interviews with retired senior military officers.

that's everyone. That is why it will grow."[23] This paper will provide greater specificity by analyzing both Russia and China as the primary great power threats executing hybrid and information warfare in the gray zone. It is essential to understand what they are doing, so that the United States not only recognizes and counters it, but also learns from it.

[23] McFate, S., *The Return of Mercenaries, Non-State Conflict, and More Predictions for the Future of Warfare*. (Go Medium Publication, Jan 22, 2019). Retrieved from: https://gen.medium.com/the-return-of-mercenaries-non-state-conflict-and-more- predictions-for-the-future-of-warfare-7449241a04e5.

Great Power Analysis

Russia's Renewed Military Thinking

Russia has invested in utilizing all aspects available within society, federal or private, legal or illegal, to conduct hybrid warfare. Their most well-known cases span over a decade from the 2007 cyber-attacks in Estonia, the 2008 intrusion in Georgia, the 2014 conflict in Ukraine, and their more recent efforts in Syria. In the NATO Research Paper, *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control States*, the author Can Kasapogulu argues "the right panacea would not be centered on the question of 'how to confront the Russian hybrid warfare challenge;' rather, the question of 'how to best understand the Russian hybrid warfare challenge."[24] The focus of this section is to evaluate previous research and how Russia incorporates SOF and alternative elements of society to shape the geopolitical arena to gain political power.

Following the collapse of the Soviet Union, a wave of privatization expanded across Russia's landscape. It acted as a catalyst for Russia to reinvent its national security strategy through the privatization of warfare—leveraging to a large extent private military companies and illicit networks that grew much out of the rise of the Vory.[25] Russia employs sophisticated political, economic, and military campaigns that combine discrete actions, and they harness the information environment to shape perceptions, opinions, and ultimately decisions. Russia is patient and content to accrue strategic gains over time—making it harder for the United States and Western allies to respond. Such actions are calculated to achieve maximum effect without provoking a direct military response from the United States or NATO, as Article 5 stipulates. Furthermore, as the United States information warfare efforts dissolved, Russia invested and expanded theirs. They

[24] Kasapoglu, Can. *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*, (NATO Defense College Rome, November 2015). *Retrieved* from https://www.files.ethz.ch/isn/195099/rp_121.pdf , 11.
[25] Galeotti, Mark. The Vory: Russia's Super Mafia, (Yale University Press, 2018).

did this through centralized control of television stations, shifting to a position of subversive control over Russian news outlets, and utilized social media bots and trolls and other emerging forms of communication to take a competitive advantage in the information environment. As these incremental gains were realized, over time, a new status quo emerged.[26]

Russia developed a near-abroad strategy to project power and influence outside its borders.[27] General Gerasimov, current Chief of the General Staff of the Armed Forces of Russia, argued that "the role of non-military 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."[28] In essence, he is describing what the United States has articulated in a whole-of-government approach to national strategic objectives—leveraging similar non-kinetic means in diplomatic, information and economic instruments of national power. Russia has extended its hybrid approach to encompass not just a whole-of-government but a whole-of-society. In which General Gerasimov's thought piece published in *The Military-Industrial Courier*—that some refer to as the *Gerasimov Doctrine*—expounds on. The basis of it incorporates the use of active measures, both overt and covert, across multiple domains. Russia then shapes and performs behavioral conditioning of a target population before commencing operations to accomplish their objectives.[29]

Russia has expanded the traditional roles and mission of SOF more so than the West. Dr. Spencer Meredith of the National Defense University gave a brief on *Countering Russian Strategic*

---

[26] *National Security Strategy of the United States of America*, 28.
[27] Steder, Frank. *Introduction, The Theory, History and Current State of Hybrid Warfare*, (Combating Terrorism Exchange, November 2016). Retrieved from https://globalecco.org/documents/327413/327631/Vol+6+No+4.pdf/, 12.
[28] Bartles, Charles. *Getting Gerasimov Right*, (Military Review, January-February 2016). Retrieved from https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/194973.
[29] Kramer. *Russian General Pitches 'Information' Operations as a Form of War.*

Approaches: Special Operations in Hybrid Warfare that captured Russia's Special Operations capabilities, which reflect a comprehensive hybrid warfare strategy using diverse entities:

- *Spetsnaz – direct action/reconnaissance, becoming more unconventional warfare capable*
- *Private Military Companies – technically illegal, but vagary gives plausible deniability and an outlet for intra-elite politics*
- *Non-state actors – most effective within democratic systems and are integrated with information operations and cyber*
- *Violent Extremist Organization proxies, puppets, partners – expand the strategic game and raise costs to the United States*
- *Competition regarding regional military commands and GRU (Russia's main intelligence directorate) control*
- *"SOF" support – limited capabilities but expanding*[30]

To broaden the effectiveness of their hybrid warfare approach, Russia blends standard overt signatures of Spetsnaz conducting traditional special operations, along with private military companies, illegal networks, and cyber capabilities. Dr. Kiril Avramov, professor at the University of Texas at Austin, describes the modern Russian soldier as one who operates in the gray zone being between a serviceman, mercenary, or spook.[31] A great example of this is Russia's ISIS Hunters in Syria. This unit provides Russia the ability to conduct military operations without overtly placing Russian troops in contested areas that could potentially escalate the conflict between great powers. [32]

---

[30] Meredith, Dr. Spencer. *Countering Russian Strategic Approaches: Special Operations in Hybrd Warfare,* (National Defense University, June 2019). Retrieved from https://nsiteam.com/social/wp-content/uploads/2019/06/Countering-Russian-Strategic-Approaches-SMA-JUN-2019-SBM-converted.pdf, 8.
[31] Avramov, Kiril and Ruslan Trad. *An experimental playground: The footprint of Russian private military companies in Syria,* (The Defense Post, February 17, 2018) Retrieved from https://thedefensepost.com/2018/02/17/russia-private-military-contractors-syria/.
[32] Avramov. *An experimental playground.*

Russia's use of non-state actors, such as the Russian Wagner Group, creates an ambiguous hybrid of privatized, yet, state-driven foreign policy.[33] To complicate matters further, Russia's execution of information operations and cyber-attacks through private companies like Sofacy, Tsar Team, and Sandworm, provide Russia the ability to fluidly impact elements in the near-abroad without confrontation from other state actors.[34] In Syria, Sudan, and the Democratic Republic of the Congo, Russia uses private military companies to carry out Russian foreign interests while providing the Kremlin plausible deniability. Exporting this hybrid model should not be taken lightly, it is blurring the lines and contesting international law in ways that pose a significant challenge for states to respond appropriately and in concert with the treaties and laws established in the current international system.

Illegal activities and their associated networks are an asymmetric advantage Russia exploits to advance their near abroad strategy. Mark Galeotti, renown Russian expert, describes how Russian "businesses and politicians alike use many methods that owe more to the vorovskoi mir than legal practice."[35] In Galeotti's book, The Vory, he captures just "how far the values and practices of the Vory have come to shape modern Russia."[36] Unlike the United States' adherence to the rule of law, Russia's exploitation of current norms and the use of alternative networks (e.g. illicit) provides them maneuverability, around sanctions for example, and freedom of action. In many ways, this is most effective against open and free societies because they run counter to the United States and Western values. Russia's operations in transnational organized crime is another

[33] Due-Gundersen, Nicolai. *Putin's Mercenaries Are Using Syria as a Training Ground*, (Lobe Log, August 20, 2019). Retrieved from https://lobelog.com/putins-mercenaries-are-using-syria-as-a-training-ground/.
[34] Sussman, Bruce. *Make It a Dozen: New Lit of Hacker Names Russia Is Using in Cyber Attacks*, (Seguro Group Inc, October 4, 2018). Retrieved from https://www.secureworldexpo.com/industry-news/russia-government-hacker-names.
[35] Galeotti, The Vory, 5. Vorovskoi mir or the so called 'thieves world' is the general term for a member of the Soviet underworld.
[36] Galeotti, The Vory, 5.

opportunity for them to wage hybrid warfare against the current world order. The criminal state of their influence focuses on public corruption. Counterfeit and contraband to include drugs, humans, weapons, and timber, for example, has increased considerably with globalization to a level that surpasses the threat from international terrorism.[37] These illicit organizations work in regular markets while utilizing the established logistics and nodes also to run illicit activities. In the case of Russia, it allows for the state to leverage these companies for state-sponsored illicit activities, circumventing sanctions imposed by the United States. However, the real concern is how these illicit networks also infiltrate public positions, businesses, and security offices in other countries, which over time, has the potential to reconfigure the nature of the state political and economic system, as in Moldova.

Like the West, Russia's covert action is based on the principle of plausible deniability. However, in more recent years, Russia has reshaped efforts in the gray zone towards a strategy of implausible deniability. Though the intent of covert action is the ability to deny knowledge of or the responsibility of an event, taking on an implausible deniability position creates further ambiguity in international affairs. Rory Cormac and Richard J. Aldrich define in *Grey is the New Black*, implausible deniability as "open secrecy"—unacknowledged interference in the affairs of others.[38] In the age of fake news and misinformation, this can be a considerable advantage. Cormac and Aldrich list two essential concepts regarding implausible deniability. "First, implausible deniability opens a gap in the decision-making of cumbersome institutions like NATO that Russia can exploit. Second, ambiguity and implausible deniability allow the construction of powerful narratives. Knowledge of Russian activity—without acknowledgement—allows the Kremlin to

[37] Miklaucic, Michael and Moises Naim. *The Criminal State.* (National Defense University Press, 2013), 153.
[38] Cormac, *Grey is the new black.*

cultivate an image of omnipotence."[39] The ultimate result is to influence decision-making in a direction favorable—or at least not harmful—to the Kremlin.

Russia tested and refined its hybrid warfare strategy throughout multiple conflict engagements. In 2008 Russia reemerged in a hybrid warfare obtrusion into Georgia. The lessons they learned there were refined and employed once again in Ukraine, where they carried out more direct combat support roles and orchestrated implausible deniability actions in Crimea. Russia perfected this strategy in Syria to the point where they realized they could export it globally in a more organized way.[40] General Gerasimov cited the Syrian civil war—a combination of an expeditionary force supported by information operations—provided the lessons to expand Russian national interests beyond its borders.[41]

Russia has since exported its hybrid warfare strategy across Africa and South America. In one case, Russia employed Spetsnaz forces across the beach of Libya in support of Khalifa Haftar, leader of the Libyan National Army. Along with strategic messaging in support of Haftar, Russia provided security for him as well as strategic messaging.[42] Though the United States openly supported the new Government of National Accord for Libya following the collapse of Muammar Gaddafi, there was continued debate within the United States government if this was the right political alignment. Until President Trump's Tweet in 2019, does the United States position appear to shift in support of Haftar. A form of strategic messaging that could be confused with the underlying diplomatic view of whether the United States supports Haftar or the Government of

---

[39] Ibid.
[40] Interview with Professor Kiril Avramov.
[41] Kramer. *Russian General Pitches 'Information' Operations as a Form of War.*
[42] Meredith III, Spencer Dr. *Countering Russian Strategic Approaches: Special Operations in Hybrid Warfare*, (National Defense University, 2019). Retrieved from https://nsiteam.com/social/wp-content/uploads/2019/06/Countering-Russian-Strategic-Approaches-SMA-JUN-2019-SBM-converted.pdf.

National Accord. This is just another example where Russia and the utilization of Spetsnaz have contested United States geopolitical influence in the information environment.

In closing, the Soviet idea of hybrid and information warfare is more complex than Western equivalents. It offers a holistic approach, adopted and implemented by a variety of public and private, legal and illegal organizations. Covert methods and actors mutually support their overt counterparts, making them deliberately difficult to conceptualize and counter.[43] Targeting the adversary's decision-making is the ultimate objective—to obtain the freedom of action to expand their national interests—short of a conventional war. Oscar Jonsson and Robert Seely, in *Russian Full-Spectrum Conflict: An Appraisal After Ukraine,* argue Russia's execution of full-spectrum conflict depends on centralized command and control that is highly coordinated.[44] They conclude Russia's comparative advantage is their ability to effectively target the European Union and NATO's cumbersome decision-making process.[45] Russia's approach is complex and concerning. However, to understand the reemergence of greater power competition and how the United States can organize against it, is incomplete, without understanding a bit of China's great power competition strategy.

The Rise of Sun Tzu in China

China's strategy, falls too, under the umbrella of hybrid warfare—its ends, ways, and means remain similar with great power competition strategies. There has been a consistent blend

[43] Cormac, *Grey is the new black.*
[44] Johnson, Oscar and Robert Seely. *Russian Full-Spectrum Conflict: An Appraisal After Ukraine,* (The Journal of Slavic Military Studies, Volume 28 2015). Retrieved from https://www.tandfonline.com/doi/abs/10.1080/13518046.2015.998118.
[45] Berg-Knutsen, Espen. *From Tactical Champions to Grand Strategy Enablers: The Future of Small-Nation SOF in Counter-Hybrid Warfare,* (Combating Terrorism Exchange, November 2016). Retrieved from https://globalecco.org/documents/327413/327631/Vol+6+No+4.pdf/, 62.

of conflict for decades they refer to as "peacetime-wartime integration."[46] China has been shaping the geopolitical landscape through informatized local wars—regional conflicts defined by real-time, data-networked command and control and precision strike.[47] Their modern framework, known as *Three Warfares*, was inspired by the underlying principles of Mao Zedong. Mao stated those favorable of the strictly military view:

> "Think that the task of the Red Army…is merely to fight. They do not understand that the Chinese Red Army is an armed body for carrying out the political tasks of the revolution. The Red Army fights not merely for the sake of fighting but in order to conduct propaganda among the masses, organize them, arm them, and help them to establish revolutionary political power."[48]

The purpose of the Red Army was not necessarily to confront the enemy in direct combat, but rather to shape conditions favorable to the political end Mao envisioned. As Sun Tzu inspired, "the supreme art of war is to subdue the enemy without fighting."[49] Today we see similar sentiments under China's information warfare strategy and it's roll in the South China Sea—shaping views on Taiwan, the One Belt One Road initiative, and the latest SARS-CoV-2 pandemic.

Chinese military writings over the past decade have centered on information warfare. They believe "achieving information superiority is seen as the precondition for achieving and maintaining battlefield supremacy," as presented in Timothy Walton's *China's Three Warfares* article.[50] They actively exploit information operations concepts as a means to direct influence on

---

[46] China's Evolving Military Strategy, p. 197

[47] Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019.* Retrieved from https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

[48] Tse-tung, Mao. *On Correcting Mistaken Ideas in the Party*, (Maoist Documentation Project, 2004). Retrieved from https://www.marxists.org/reference/archive/mao/selected-works/volume-1/mswv1_5.htm.

[49] Sun Tzu translated by Thomas Cleary. *The Art of War,* (Shambhala, January 11th 2005).

[50] Walton, Timothy. *China's Three Warfares,* (Delex Systems Inc., January 18, 2012). Retrieved from https://www.indianstrategicknowledgeonline.com/web/Three%20Warfares.pdf.

the engagements and outcomes in areas of strategic competition.[51] China has since formalized its strategy, known as *Three Warfares,* to gain political power through three main principles: psychological warfare, public opinion (media) warfare, and legal warfare.

Psychological warfare intends to influence foreign decision-makers and how they approach their policies on China through the coordinated use of propaganda. China's intent is to target critical nodes in foreign government decisions to achieve non-linear effects. Walton describes China's thinking related to their adversaries, "the enemy's motivation and willingness to wage war could be targeted, by eliminating opposing leadership, diminishing international support, undercutting military capabilities, affecting the economy, or sowing domestic political dissent."[52] A retired senior military officer and current professor at the University of Texas at Austin recalled a conversation with Chinese business professionals who mentioned China spends a considerable amount of time and resources focused on United States decision making. China is sharply attuned to the core definition of information warfare.

Public opinion, or media, warfare aims at shaping and influencing domestic and international public opinion through both overt and covert media manipulation. A vital component of this is China's United Front Work Department. Peter Mattis, writes for War on the Rocks and in *The Third Magic Weapon: Reforming China's United Front,* states the United Fronts' purpose is to "rally social groups and individuals to support the Chinese Communist Party (CCP) and its objectives."[53] Efforts are focused on the behavioral conditioning of the domestic population. The People's Liberation Army (PLA) routinely sends "significant media teams to cover the efforts and

---

[51] Raska, Michael. *Hybrid Warfare with Chinese Characteristics*, (ETHZurich, January 20, 2016). Retrieved from https://css.ethz.ch/en/services/digital-library/articles/article.html/195268/pdf.
[52] Walton, *China's Three Warfares,* 5.
[53] Mattis, Peter and Alex Joske. *The Third Magic Weapon: Reforming China's United Front,* (War on the Rocks, June 24, 2019). Retrieved from https://warontherocks.com/2019/06/the-third-magic-weapon-reforming-chinas-united-front/.

inform the population of the PLA's, People's Armed Police's, and militia's work in non-traditional security missions."[54] Domestically focusing on the information environment allows China to influence local sentiment and develop favorable domestic support for both domestic and international strategic actions.

Legal warfare, or "Lawfare," seeks to shape the legal context and justification for Chinese foreign policy action.[55] Nowhere is it better illustrated than in the South China Sea and the contested islands China is developing and claiming as sovereign territory. Additionally, we can see this strategy take place across China's One Belt One Road initiative. China's economic pursuits, bound by a legal framework, create enduring influence as shown in Sri Lanka, Pakistan, and elsewhere across the Eurasian landmass and littoral. It is practically written into the law for Chinese businesses to support the CCP. China's National Security Law, enacted in 2015, states that its citizens and corporations have the "responsibility and obligation to national security."[56] To this point, the 2017 Chinese National Intelligence Law states Chinese companies must "support, assist, and cooperate with China's intelligence-gathering authorities."[57] Though the law is vague, some experts and United States officials highlight that the Chinese telecommunication company, Huawei, for example, could be forced to help the CCP with intelligence gathering.[58] Authorizing Huawei access to the telecommunication infrastructure for the United States and Western allies is contested. This is not to diminish its competitive advantage economically, but because it would

---

[54] Walton, *China's Three Warfares,* 8.
[55] Mattis, Peter. *China's 'Three Warfares' In Perspective,* (War on the Rocks, January 30, 2018). Retrieved from https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.
[56] Chinese National People's Congress Network. *National Intelligence Law of the People's Republic,* (June 27, 2017). Retrieved from http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.
[57] Ibid.
[58] Maizland, Lindsay and Andrew Chatzky. *Huawei: China's Controversial Tech Giant,* (Council on Foreign Relations, February 12, 2020). Retrieved from https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

give them a critical point of leverage on the telecommunication infrastructure they could shut down at a moment's notice, crippling the United States or any adversary.

To be clear, we are not talking about doctrine, but rather the strategy China intends to utilize to gain a competitive advantage. This strategy is often related to the PLA, but Peter Mattis characterizes it as the overarching way in which the CCP approaches influence operations and active measures, just their normal way of doing business.[59] Another way China implements this strategy is by identifying select foreign political, business, and military elites and organizations abroad relevant to China's interests. In another Taiwan example, a local Taiwanese media described a high-level espionage case that involved a senior Taiwanese military officer in the Military Intelligence Bureau, who collected operational military intelligence for China.[60] The U.S. Department of State *2019 Country Reports on Human Rights Practices* identified PRC officials who used the fourth Beijing-Taiwan Media Forum to shape Taiwan media outlets coverage in support of Chinese political priorities. China's influencing of the domestic population could impose tensions with Taiwanese political leadership.[61] Though, Taiwan is not the only one vulnerable to China, who has also attempted to recruit American spies through LinkedIn and other social media platforms.[62] Ultimately, China tailors its network analysis to influence operations that may include conversion, exportation, or subversion.[63]

---

[59] Mattis, Peter. *Contrasting China's and Russia's Influence Operations,* (War on the Rocks, January 16, 2018). Retrieved from https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations/.
[60] Hsiao, Russell. *War Without Gunfire: China's Intelligence War with Taiwan,* (The Jamestown Foundation, November 5, 2010). Retrieved from https://jamestown.org/wp-content/uploads/2010/11/cb_010_239049.pdf?x12088.
[61] Department of State Bureau of Democracy, Human Rights, and Labor. *2019 Country Reports on Human Rights Practices: Taiwan,* (Department of State, 2019). Retrieved from https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/taiwan/.
[62] Wong, Edward. *How China Uses LinkedIn to Recruit Spies Abroad.*, (The New York Times, September 27, 2019). Retrieved from https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.
[63] Raska, *Hybrid Warfare with Chinese Characteristics.*

China's information warfare strategy is carried out by multiple government agencies, but primarily the PLA. Unfortunately, there was little information on how China employs its SOF in support of its *Three Warfares* strategy. However, that is not to say they are not learning from Russia's employment of SOF or even the United States to shape events. There should be no surprise if bread crumb trails of Chinese SOF appear in places like Taiwan, Hong Kong, and remote areas of Africa in the future.

The most recent example of Chinese *Three Warfares* at play, across all concepts of propaganda, public opinion, and legal warfare, is the SARS-CoV-2 pandemic. Multiple narratives originated from China that had global implications. First and foremost is the lack of transparency and censorship that occurred during the outbreak. For example, "China's leader, Xi Jinping, reportedly spoke on the issue before the Politburo Standing Committee on January 7, two weeks before he mentioned it publicly."[64] Another example of how China is shaping its public opinion is the narrative Chinese elite claimed, that the United States military brought the SARS-CoV-2 virus to China during the October 2019 Military Olympics in Wuhan.[65] Though this is unlikely to gain any traction in the United States or with Western allies, it does play a factor in the perceptions of the people of China and more regional Asian nations. From a propaganda standpoint, China is doing everything they can to save face by nearly rewriting the history of the virus and grooming the elements of the language around it.[66] Respectively, China has issued a new policy, in which all academic papers on SARS-CoV-2 require extra vetting before public dissemination—specifically,

---

[64] Veron, Emmanuel and Emmanuel Lincot. *Debate: How Beijing is trying to save face in the global fight against Covid-19,* (The Conversation, April 2, 2020). Retrieved from https://theconversation.com/debate-how-beijing-is-trying-to-save-face-in-the-global-fight-against-covid-19-134996.

[65] Myers, Steven Lee. *China Spins Tale That the U.S. Army Started the Coronavirus Epidemic,* (The New York Times, March 17, 2020). Retrieved from https://www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html.

[66] Veron, *Debate: How Beijing is trying to save face in the global fight against Covid-19.*

studies on the origin of this virus must be approved by the CCP.[67] The competing narratives that emerge, will impact policymakers and public opinions for years to come.

Peter Mattis' article, *China's Three Warfares in Perspective*, describes China's efforts as the way the "PLA decided to conceptualize the different tasks of shaping the environment in which the army operates."[68] This shaping of the operational environment through hybrid and information warfare strategies, that both Russia and China employ, in many ways, was learned by studying and mirroring the United States. In one case, Operation QRHELPFUL, is a historical example and the most recent declassified information warfare covert action to date that is evaluated in the following section. Then a more recent and empirical model will be discussed focusing on the principles of understanding and utilizing the information environment as the main effort in a combined joint military operation. The intent is to understand and identify general principles and lessons learned from former and more recent United States information operations that can be applied today to more effectively organize and execute hybrid and information warfare against great powers.

---

[67] Gan, Nectar, Caitlin Hu and Ivan Watson. *Beijing tightens grip over coronavirus research, amid US-China row on virus origin*, (CNN, April 13, 2020). Retrieved from https://www.cnn.com/2020/04/12/asia/china-coronavirus-research-restrictions-intl-hnk/index.html?utm_term=15867740039112da675e3714f&utm_source=Five+Things+for+Monday%2C+April+13+2020&utm_medium=email&utm_campaign=197814_1586774003917&bt_ee=7duN7Y0HOV7TpCOR%2Fbq6enmoFq0G90rKIbZYMuyBMw1cTqSCewmNfo9KiZJqGLMN&bt_ts=1586774003917.

[68] Mattis, *China's 'Three Warfares' In Perspective.*

Historical and Recent U.S. Information Warfare Examples

Operation QRHELPFUL

The United States during the Cold War conducted information warfare through entities like USIA, U.S. Agency for International Development, the DoD, DoS, and the CIA.[69] It required a whole-of-government approach to counter the former Soviet Union. The most recent example, due to declassified government documents of a United States information warfare campaign against a great power, is Operation QRHELPFUL. Seth Jones' uncovers the details of this operation in his book and shares his comments about Operation QRHELPFUL at an event sponsored by the Intelligence Studies Project held at the University of Texas at Austin in April 2019.

In 1981, a surge of labor unrest in Poland created an opportunity behind the Iron Curtain for the CIA to execute an aggressive information warfare campaign. Lech Walesa, a charismatic union leader at the Gdansk shipyard, captured the support of nearly 10 million laborers to rise against industrial injustice and horrible living conditions in Poland—this trade union became Solidarity. After his election, President Ronald Reagan held multiple National Security Council meetings regarding the rising tensions in Poland between a pro-democracy labor movement and the communist regime. The CIA's intelligence analysis stated, "Poland presents the USSR with the most threatening and complex challenge to its vital interests to emerge in the postwar period."[70] The CIA predicted the Soviets would force the Polish regime to declare martial law in response to Solidarity. Security forces were expected to destroy property and haul Solidarity leaders to jail. This outraged President Reagan and led to a series of national security decision directives (NSDD)

[69] Robinson, L. Helmus, T. Cohen, R. Nader, A. Radin, A. Magnuson, M. Migacheva, K. *Modern Political Warfare: Current Practices and Possible Responses*. (RAND Corporation, 2018). 15.
[70] National Intelligence Estimate. *Soviet Goals and Expectations in the Global Power Arena*, (Central Intelligence Agency, July 7, 1981). Retrieved from https://www.cia.gov/library/readingroom/docs/DOC_0000268220.pdf, 15.

centered on disrupting Soviet control in Eastern Europe – NSDD-32 and NSDD-54.[71] President Reagan's alignment with the intelligence community, political top cover, and aggressive stance to counter Soviet dominance in Eastern Europe were prominent in the centralized support and overall design of Operation QRHELPFUL.

A covert action information warfare program, Operation QRHELPFUL, was initiated with a "presidential finding to provide money and non-lethal equipment to moderate Polish opposition groups through surrogate third parties, hiding the U.S. government's hand."[72] Deniability was a key factor for Solidarity members as well as the United States government. The protest movement needed to be Polish-led and orchestrated to ensure authenticity and legitimacy to both domestic and international actors. There was also significant counterintelligence risk, the Soviet Komitet Gosudarstvennoy Bezopasnosti (KGB), or Committee for State Security, had extensive source networks in Poland looking to counter the West's influence. Thus, the design of Operation QRHELPFUL was critical to ensure that any intervention by the United States was concealed. Working through third parties, establishing a surrogate network, and developing "ratlines" to funnel money and non-lethal equipment like radio antennas, was essential to support Solidarity. Additionally, advances in technology in the early 1980s enhanced the efforts of Solidarity—the CIA provided radio antennas that bypassed Soviet control of the radio spectrum. The cumulation of these efforts enabled Solidarity to print newspapers (e.g. Tygodnik Mazowsze, which means weekly of Mazovia, a region in central Poland), broadcast radio messages, and disseminate other propaganda materials to shape their narrative and build popular support.

[71] Jones, Seth G. *Covert Action: Reagan, the CIA, and the Cold War Struggle in Poland*. (W.W. Norton Inc., 2020). 301.
[72] Jones, *A Covert Action*, 301.

After nearly eight years of shaping perceptions, opinions, and decisions, Operation QRHELPFUL efforts were realized in the 1989 Polish elections with approximately 75-80% in favor of the trade union's candidates.[73] It is difficult to ascertain how influential Operation QRHELPFUL was in countering the Soviets. The United States was simultaneously waging information warfare across Europe, supporting ideological values of democracy and freedom through entities like Radio Free Europe and other forums. However, Operation QRHELPFUL would have had a multiplying effect with other organizations like the National Endowment for Democracy and the Catholic Church, who aided Solidarity through coordination and gaining efficiencies across their respective areas of influence. Scholars may debate how important all of this was, but Solidarity winning the votes in Poland was critical to ending communist rule across Eastern Europe.

Jones describes some of the main tenants of Operation QRHELPFUL were financial support, a technological component, and masking the United States involvement. This enabled Solidarity to gain legitimacy, print newspapers, broadcast radio programs, and conduct a wide range of information operations against the Soviet-backed government.[74] Part of a successful information warfare effort then must include the highest levels of governmental support, resources or money, non-lethal equipment/aid, technological advancements, and deniability that creates authenticity and legitimacy for the narrative and cause.

In the following section is a recent example where information, used as the main effort, conditioned the operational environment for a combined joint military operation in the Middle

---

[73] Tagliabue, John. *Big Solidarity Victory Seen in Poland,* (The New York Times, June 5, 1989). Retrieved from https://www.nytimes.com/1989/06/05/world/big-solidarity-victory-seen-in-poland.html.

[74] Clements Center for National Security. *Russian Active Measures and the U.S. Response: Lessons from the Cold War*, (Clements Center, April 23, 2019). Retrieved from https://www.clementscenter.org/events/item/1633-a-conversation-with-seth-jones.

East. Real-world polling data was utilized to conduct a psychographic analysis of the human terrain—tailoring tactical to strategic messaging to shape perceptions and condition behavior—while working through a legitimate regional partner. This approach resembles Russia's hybrid and information warfare operations in Georgia and then Crimea at the beginning of the 21st century—testing this operational methodology, learning from it, and enhancing these capabilities to accomplish national strategic objectives. Due to the sensitivity of the area of operations, some of the unclassified information was modified.

Information as the Main Effort

What follows is an example of enabling regional partners who have a local affiliation to shape an appropriate narrative in support of counterterrorism operations. The 2017 *NSS* Priority Action to information statecraft requires activating local networks. It stated "local voices are most compelling and effective in ideological competitions. We [US] must amplify credible voices and partner with them to advance alternatives."[75] Messaging can be the United States' most effective weapon, but broad messaging is largely ineffective and can be counterproductive if it activates the adversary's networks.

The operational design for this information warfare effort utilized a model where the main aim was more inclusive of understanding the operating environment. It incorporated the human domain and used information warfare characteristics to shape the decisions and behaviors of locals through similar components that made Operation QRHELPFUL successful support from leadership, resource assistance, incorporation of technology and data, and minimizing the United States signature. The objective was to set conditions with the local populace to establish a behavior

[75] 2017 *National Security Strategy of the United States of America*, 11.

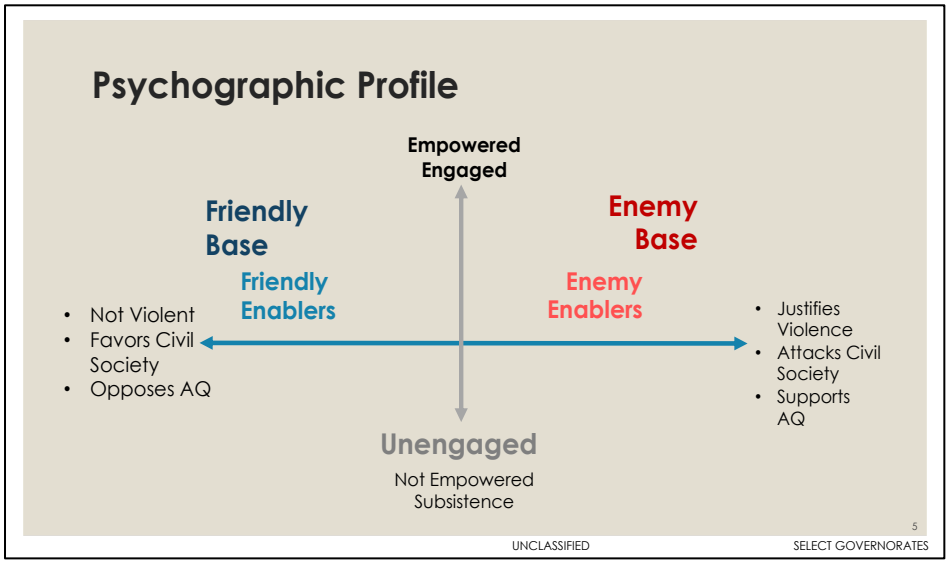
that divided hardcore extremists from potential supporters while favoring foreign military efforts in the region. The unofficial terminology utilized in this section to describe this approach is the Base/Enabler Methodology (B/EM). The intent was to shape both the base and enemy's perceptions, decisions, opinions, and behavior.

The B/EM can be softly defined as segmenting apart those who support peaceful civil society from those who support acts of violence. It provides an operational framework to clarify strategic messaging opportunities. The B/EM analysis requires thinking through the strategic goals of the engagement and weighing the impact of actions—kinetic, non-kinetic, and no-action—on the groups that will strengthen civil society and those who would overthrow it. Based on other operational experiences in South Asia, East Africa, North Africa, Latin America, and the Middle East, a correlation exists between indicator messaging and network activity on the ground.

The following figures, tables, and data throughout this section illustrate findings from utilizing polling results on security issues in Yemen from a March 2017 Yemen Polling Center for the European Union and a CENTCOM commissioned survey from May-August 2018.

All the preparatory work was focused on civil society and shaping the human domain, as condition setting is a critical component in an information warfare model. In this case, the methodology conducted a psychographic analysis and segmented the local population to create a tailored influence operation, as outlined in Figure 1. The intent was to shape local conditions to enable a follow-on SOF advise and assist mission. It required identifying friendly and enemy base and enablers, as well as those unengaged. This methodology provides an operational framework to influence and counterinfluence through identifying opportunities for strategic to tactical messaging aligned with the associated or desired impact.

Figure 1. Psychographic profile of the Base/Enabler Methodology



It is most useful to segment the population into operational "Friendly" and "Enemy Enabler" groupings. The goal of civil society engagement is to build friendly networks and suppress enemy enablers. In Yemen, that means finding supporters of peace and civil society norms from within both the Sunni and Zaydi populations and messaging—both directly and with indicator messaging—to reach them.[76] In Yemen, we used the polling survey results to segment

[76] Cooperation within the US interagency helped identify the appropriate tribal elements in which to focus messaging.

the population into the following groups: Friendly Base, Friendly Enablers, Unengaged, Enemy Enablers, and Enemy Base.

Table 1. Segments of Base/Enabler Methodology

Friendly Base: • Strongly opposed to violence • Opposed AQAP • Self-directed and engaged in society **Friendly Enabler:** • Mostly opposed to violence and AQAP • Somewhat engaged	**Unengaged:** • Feel others control their lives **Enemy Enabler:** • Some support for violence • Some support for AQAP • Somewhat engaged **Enemy Base:** • Support AQAP or violence

The purpose was to understand what statements were most effective to shape the narrative and who to target what statements towards. After analyzing the data in Table 2, it was shared with the lead regional partners—who were viewed as credible and could engage more effectively at the local level than United States forces to shape the information environment in support of future operations.

Table 2. Segment characteristics

Friendly Base	• Mostly men (72%), more empowered, feel strongly supported & cared about
	• Watch al Arabya TV
	• Pro-West
Friendly	• More Males (52%)
Enablers	• Financially strained
	• Highest Education Levels
Enemy Base and	• Many Unemployed, less educated
Enablers	• Younger, more likely to live with parents
	• Mixed on West; more likely to watch BBC
Unengaged	• Majority of this group is women
Houthis	• More likely to work full time
	• Most anti-US group

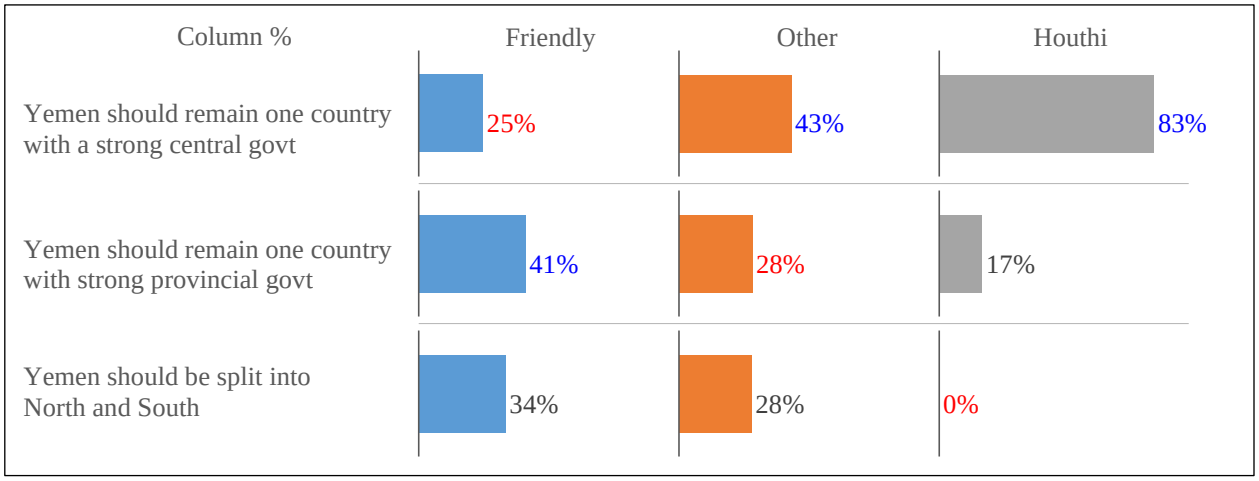
How to reach the targeted populations varied. The Yemenis gather multiple sources of information, from international satellite channels to neighborhood friends and family. Local television channels reflect the viewpoints of their host cities: Sunni and Shi'a, north and south. This fragmented media environment can make information gathering difficult, but it also allows discrete communications targeted geographically or demographically. The United States and its partners have active information operations in Yemen, as well as many attributable channels for communicating both inside Yemen and to the global media. Successful messaging is achievable if the relevant and acceptable message is delivered by a trusted messenger—as in the case with the Solidarity movement in Poland. Messages attributable to the United States, either directly or indirectly, are likely to be received poorly. Although many Yemenis have positive feelings about aspects of the West, and almost 70% would, for example, be happy to have their children study in the West—they are broadly opposed to the United States interference in the internal politics of Yemen. Seventy percent of Yemenis in the selected area say the United States role in Yemen internal affairs is negative. This compares to 83% with negative feelings towards Iran, and 39% negative towards the regional partner (with 46% positive towards regional partner).

In the selected areas of Yemen, the most impactful telecommunication medium is television, with other sources of communication falling far behind. Overall, radio and newsprint are used by only small minorities. Television penetration is strong both through local channels and international channels. Facebook and other social media venues will reach only a small percent of the population. There is some variation among the segments in which channels or stations are accessed. With the Houthis, al Maseerah is most popular (45%), along with local channels. For the other segments, Friendly and Enemy, al Arabya is the most watched, followed by Aden TV, Suhile TV, and al Jazeera. Enemy Enablers were somewhat more likely to watch BBC than other

segments, but it is still a small group (6%). Survey respondents said they have the most confidence in their local imam, Red Crescent, local government, and police. They have the least confidence in the Houthis, AQAP, President Hadi, elections, and the tribal justice system. Tribal elders (45%), community leaders (32%), imams (12%), police and political leaders (4%) were said to be the most influential in the local community, based on a normalized scale.

The most substantial concern of Yemenis is the war (31%), but enemy groups and Houthis each rate other issues as bigger concerns. For enemy groups, corruption is more important, and for Houthis rising prices and Al-Qaeda in the Arabian Peninsula (AQAP) matter more than the war. On a personal and family level, the concerns are more prosaic; jobs, running water, and electricity top the concerns. Safety and security are further down the list. In addition to a dislike for Iranian and United States interference, there were also divided views about what the government should look like should peace come, as identified in Figure 2.

Figure 2: Opinions on Yemen's governmental structure vary



The majority supported a degree of regional autonomy, if not complete separation of North and South into two countries. As a result, the following messages were not likely to resonate with the audience segments:

- *We are fighting for a unified Yemen controlled by a strong central government.*
- *We are fighting to restore the legitimate President Hadi government.*
- *Yemen should have a secular rule of law where all people are treated equally regardless of religion.*
- *The United States is proud to sponsor this program to help Yemen.*
- *People need to reject AQAP and its violence.*

Delivery of these messages in a manner attributable to the United States can be counterproductive, motivate Enemy Enablers, and reinforce the messaging from AQAP and the Houthis. The following messages are more likely to be successful in support of the Friendly Base, as they address the concerns of Yemenis.

- *Iran and the Houthis cannot be allowed to dominate Yemen.*
- *Yemen can prosper with strong regional governments after the war.*
- *Ending the war will mean ending airstrikes, restoring the economy, and creating jobs.*
- *Yemen can have a balance with the West, bringing benefits while stopping interference.*
- *Success will bring a "peace dividend" as money will pour in for reconstruction*.
- *Success will end the airstrikes and the war.*

Additionally, the below messages could suppress the Enemy Enablers and shrink the size of their networks. It is important to note, that for much of the Enemy segment, stopping Houthi and Iranian domination are persuasive motivators. Official government forces need to be convincingly better at repelling the Houthis than other Sunni groups. It is worth noting that the Enemy segment identifies corruption as a key concern as well.

- *We want to restore order and security as soon as possible.*
- *A Republic of Yemen Government victory will defeat the Houthis and stop the airstrikes.*

- *A new government will fight corruption and funnel reconstruction funding into building water supplies, electricity to jump start jobs.*
- *A peaceful Yemen will let local people and tribes oversee their own future.*
- *Peace under the official government will connect Yemen to its proper place in the world.*
- *Iran and the Houthis cannot be allowed to dominate Yemen—locking us into permanent conflict with our neighbors and destroying our future in the world.*

Once the operational environment is understood, then look to craft the message. Every message has three parts: the source, the message, and the audience—all three are essential. Even if good themes are developed, the attribution can be wrong or even broadcasted to the wrong segment. Additionally, United States attribution, whether intentional or not, often undermines the message, so it is imperative to have message discipline through credible local voices, just as stated in the 2017 *NSS*. Local voices should be natural leaders in the community, who can amplify themes that endorse or promote the strategic narrative or policy objectives.

With this knowledge of the operational environment, the next phase is to implement the B/EM framework towards the desired objectives. In 2017, a strategic offensive in a southern Yemen province was led by the regional partner, alongside 2,000 local forces. The offensive resulted in pushing AQAP out of the province and into the nearby governorate. The regional partner's efforts to build a local security element was also critical to shaping the narrative, both strategically and tactically. Meanwhile, AQAP continued tactical and strategic messaging to shape their perception towards Enemy Enablers and others to find support for their decision to withdraw. This latter point is simply to illustrate the dynamic nature of using the information environment to shape perceptions. The following sections will discuss implications and recommendations to gain a competitive advantage with the information element of national power by harnessing a hybrid approach and executing it in the gray zone.

Implications

The 2018 *NDS* recognized the enduring strategic competition between the United States, Russia, and China requires a whole-of-government approach—diplomatic, informational, military, and economic—referred to as *DIME*. Conflict in the 21st-century has escalated within the information environment. Diplomatic, military, and economic remain significant elements, but because United States adversaries are weaker in these areas, they have tilted their strategies to leverage the information environment through hybrid warfare. Russia's use of private military companies have mirrored the United States model of employing Blackwater and other contractors throughout conflict areas.[77] China's observation of the Persian Gulf War—how the United States painted Iraq as an aggressor to build consensus and support from the international community, to include other Arab nations—shaped their information warfare strategy. This is precisely an area of geopolitical conflict that Russia and China have developed significant capabilities.

Scott Johnson, of the CIA Center for the Study of Intelligence, argues that information warfare extends beyond the techniques and capabilities for traditional forms of information warfare.[78] It has three parts to be effective: a set of information warfare elements (techniques and capabilities), a comprehensive strategy that applies and orchestrates them, and a target and objective.[79] A useful definition or model of information warfare, therefore, has to describe the ultimate target and objective, and identify and list the applicable elements of information warfare.[80] The ultimate target for Operation QRHELPFUL was bolstering a pro-democratic movement to counter the Soviets by indirectly supporting Solidarity. This was done through financial and other

[77] Blackwater was the former name of a well known US private military company, but it's name has since changed to Academi due to a public image mishap in Iraq in 2007.
[78] Johnson. *Toward a Functional Model of Information Warfare*.
[79] Ibid.
[80] Ibid.

non-lethal assistance to enable Solidarity's efforts through surrogates and ratlines across Europe. US SOF, along with interagency support to the regional partner prior to the combined joint military operation, is representative of the testing and evaluating of an operational design the Russian's pioneered in Georgia and Crimea—shaping perceptions, decisions, opinions, or the behavior of the friendly and enemy base and enablers. Unique psychographic analysis was conducted while leveraging information technologies to disseminate targeted messages. Much of the operation was possible because, like Solidarity in Poland, the regional partners provided an authentic and legitimate voice. The lessons learned in Yemen can be more broadly applicable to steady-state conflicts and great power competition.

The United States military has become a significant enabler of United States foreign policy, covering all spectrums of national power to some degree. Therefore, the United States should reframe how it conducts military operations. The narrative should become the main effort, where all other actions (overt and covert) are executed to shape the trajectory of the narrative. Major General (Ret.) Michael Flynn highlighted in *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan,* that the intelligence community must embrace open-source, population-centric information as the lifeblood of their analytical work.[81] Part of understanding what is shaping the operational environment is to incorporate all friendly and enemy acts into a common operating picture to understand what and how activities are influencing the area of operations. For example, do direct action operations ahead of a conventional clearance enhance conditions for stability or counterinsurgency, or do they increase the threat to conventional coalition members?

[81] Flynn, Michael Major General (Retired), Captain Matt Pottinger, Paul Batchelor. *Fixing Intel. A Blueprint for Making Intelligence Relevant in Afghanistan,* (Center for a New American Security, January 2010). Retrieved from https://online.wsj.com/public/resources/documents/AfghanistanMGFlynn_Jan2010.pdf, pg. 23.

How are military or interagency actions conditioning the local populace? These types of questions drive towards the effectiveness of the operation to reach United States national security objectives.

Russia and China identify the weak spots, or gray areas, between governmental organizations where national law and regulations impose limits that impact cross-agency coordination and collaboration. The 2017 *NSS* identified that "repressive, closed states and organizations, although brittle in many ways, are often more agile and faster at integrating economic, military, and especially informational means to achieve their goals. They are unencumbered by truth, by the rules and protections of privacy inherent in democracies, and by the law of armed conflict."[82] Russia's approach is to utilize the most effective means necessary to achieve their stated objective, regardless of ethics or morals they may cross. In the world we live in today, this challenges the United States, who, in some ways, is constrained by American values. When Russia more freely operates with illicit networks and human rights violators, the United States' ability to influence is diminished. This creates a dilemma for the United States and Western allies who are restrained by the very world they built to counter such influence collectively.

Crimea and the Donbas region of Ukraine, with its deployment of "little green men," namely, soldiers wearing unmarked uniforms make direct state attribution difficult. Why didn't Crimea respond the way we thought they would or should have when Russia invaded? Because Russia was conditioning the area for years. Utilizing the information environment and use of the Spetsnaz, shifting the sentiment towards, and any antibodies away, from future Kremlin action. Quite like the behavioral conditioning and targeted messaging conducted in Yemen. The idea behind the following approach falls in line with reflexive control theory. The intent was to set conditions for adversary and civil society perceptions to induce behavior favorable to a future

[82] *2017 National Security Strategy of the United States of America*, 27.

operation.[83] This framework of reflexive control theory, Kasapoglu described previously, is aligned with the B/EM model utilized in the Yemen case study.

Russia and China are ahead of the game when it comes to leveraging industry and the private sector for national security objectives. "The United States must prepare for this type of competition," as stated in the 2017 *NSS*. "China, Russia, and other state and non-state actors recognize that the United States often views the world in binary terms, with states being either "at peace" or "at war," when it is a spectrum of continuous competition."[84] Similar sentiments were echoed throughout the interviews with retired senior military officers. Senior political levels of the United States government view the conflict spectrum in black and white, but in contrast, United States adversaries operate fluidly in the gray zone.[85] Heavily influenced by then Secretary of Defense James Mattis, the 2018 *NDS* specifically addressed the need that, "we [US] must anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us, while developing operational concepts to sharpen our competitive advantages and enhance our lethality."[86] Reviewing how great powers are shaping conflict, and coupled with the United States examples utilizing hybrid capabilities within the information environment, can address an organizational concept to "sharpen [this] competitive advantage" to operate more fluidly in the gray zone. The following section will identify four overarching recommendations to organize for conflict in the 21st-century.

[83] Kasapoglu, *Russia's Renewed Military Thinking,* 5.
[84] 2017 *National Security Strategy of the United States of America,* 27.
[85] Interviews with retired senior military officers.
[86] *2018 National Defense Strategy,* 7.

Recommendations

Understanding the adversary's hybrid and information warfare strategy is a critical step in designing an organizational framework for the United States to better compete against great powers. The United States needs to return to a level of effort like the hybrid and information activities conducted during the Cold War. The following recommendations are founded on the lessons learned and principles identified in this report—conducting hybrid warfare and leveraging the information environment—while in a continuous state of conflict in the gray zone. This requires vertical and horizontal organizational efforts to include: a shift in policy, a new organizational framework, assigning a lead, and adopting a whole-of-society approach.

1. Create a policy of ambiguity and establish a working group

Without a coherent policy and corresponding strategic framework, the United States will waste time, effort, and money on unrealistic hybrid and information warfare campaigns with little to no success. The United States should develop a policy of ambiguity. As in Russia's case, the use of implausible deniability led to the increase use of special forces, creating greater freedom of maneuver between secrecy and visibility.[87] Implausible deniability allows states to communicate resolve, while not escalating crises into open warfare.[88] The intent is to generate a situation where it is unclear whether a state of war exists, and if it does, who are the aggressors and who are not.

There is a need to develop an overall coordinated effort. An initial step is to create a Joint Interagency Coordination Group (JIACG) to explore in depth an organizational design. The JIACG's charter should review the structural changes that occurred following the 9/11 attack, most of which were counterterrorism centric. Examining these changes will identify whether the current

[87] Cormac, *Grey is the new black.*
[88] Cormac, *Grey is the new black.*

organizational design needs revision to be more effective against great power competition. Who has oversight, who has accountability and who has the resources to structure such an operational entity is the challenge.[89] The United States should think about the organization and the respective entities in a systems approach that will lead the United States through this transition point and into the current conflict space. Future structures must aim at achieving greater speed and effectiveness, implementing ways and means to disrupt, counter, and execute hybrid and information warfare against great powers to meet the desired ends of the United States.

Organizational structures should consistently adapt and change for emerging threats. The United States can look to its allies for such examples. The United Kingdom's Ministry of Defense, in August 2019, restructured some organizations to confront the evolving threats emerging in cyber and information warfare. Their new organization was to provide an asymmetric edge on: "intelligence, counter-intelligence, information operations, electronic warfare, cyber and unconventional warfare."[90] Joint military commands and the interagency can come together to provide a more comprehensive capability to counter threats emanating from great power competition. The whole-of-government approach, with its unique authorities and capabilities, needs to integrate in a more operational way and to further incorporate all of society.

2. Formalize a Joint Interagency Task Force

Nation-state competitors, along with other non-state actors, are designing their strategies and organizational structures to better leverage the information environment. They are exploiting seams in international law and norms and disrupting the post-World War II order developed and

[89] Interviews with retired senior military officers.
[90] Owen, Jonathan. *British Army ramps up information warfare capability to meet 21st-century threats,* (PR Week, August 6, 2019). Retrieved from https://www.prweek.com/article/1593186/british-army-ramps-information-warfare-capability-meet-21st-century-threats.

led by the United States. These threats span across the interagency and make it difficult for thorough analysis and effective responses without the proper integrated targeting and operational cells to identify, protect, and counter threats, such as cybercrime, financial crimes, and state-sponsored illicit activities.[91] Establishing a Joint Interagency Task Force is recommended for something as strategic as countering Russian or Chinese hybrid and information warfare. This requires a national charter to layout the authorities, members, and resource requirements.[92] JIATFs are a proven organizational framework to help mitigate asymmetric threats.

JIATFs were extensively used throughout the last two decades in the Global War on Terror. They form when a mission requires exceptionally close integration of two or more United States government agencies.[93] They are also traditionally utilized to increase interagency sharing, but they should adapt and change to do more than fuse intelligence and information. Rather, executing the authorities and capabilities brought by the whole-of-government. The current JIATF construct is not fully operationalized, and it should develop a greater role when executing or countering hybrid and information warfare.

This is likely to meet considerable friction if the chain of command remains structured in traditional ways. JIATFs are designed to operate external to the traditional governmental structure, and transcend the internal capabilities and authorities of Combatant Commands and Joint Task Forces, as stipulated in the *Joint Forces Operations and Doctrine* publication.[94] Historically, command and control is assigned to the Secretary of Defense, however, this could shift based on

---

[91] Center for Complex Operations Institute for National Strategic Studies. (2013). Convergence: Illicit Networks and National Security in the Age of Globalization. Washington D.C.: National Defense University Press. p. 241.

[92] *Joint Interagency Task Force publication,* (The Lightning Press, 2020). Retrieved from https://www.thelightningpress.com/joint-interagency-task-force-jiatf/.

[93] Ibid.

[94] *Joint Interagency Task Force publication,* (The Lightning Press, 2020). Retrieved from https://www.thelightningpress.com/joint-interagency-task-force-jiatf/.

the agreement in a memorandum of understanding and specific mission requirements. The intent is to increase cooperation and collaboration across the whole-of-government, and to limit the bureaucracy through decentralized authority and responsibility. This would enable a response at the speed and scale in which the likes of Russia and China leverage due to their authoritarian regimes. The purpose is "to close the gap which now exists between State and Defense at the program level and to ensure that our [US] political, propaganda, economic and military efforts are properly related to each other."[95] Bringing together the instruments of national power at the National Security Council level alone is no longer sufficient. Whole-of-Government efforts should be pushed down to lower echelons to operationalize the full-spectrum of government capabilities.

3. An organization to initially lead the effort—SOF

There is currently no United States agency that has the lead conducting hybrid or information warfare. Though, there is no single DoD element that can meet all the requirements to be effective in conducting hybrid warfare, the Special Operations Command (SOCOM), who has led many effective JIATF's with counterterrorism missions, is an acceptable place to start. Dr. Michael Vickers, former Under Secretary of Defense of Intelligence, stated, "I want as much influence around the world as I can; the main competition [is] where SOF lives." [96] Admiral (Ret.) William McRaven, while the Commanding General of the Joint Special Operations Command, expressed the idea that "SOF are best used in the tenuous space between diplomacy and conventional war."[97] Thus, SOF should play a strategic and operational role in conducting hybrid

[95] Bridging the Gap, p. 55

[96] Taft, John, Liz Gormisky and Joe Mariani. *Special Operations Forces and Great Power Competition*,(Deloitte, June 17, 2019). Retrieved from https://www2.deloitte.com/uk/en/insights/industry/public-sector/future-of-special-operations-forces-great-power-competition.html.

[97] Bernd Horn, J. Paul de B. Taillon, and David Last, Force of Choice: Perspectives on Special Operations (Montreal: McGill-Queen's University Press, 2004).

and information warfare—combined with other instruments of national power to harness unique ideas and resources to adapt to the changing nature of warfare. This is not too different than what SOF already does around the globe conducting counterterrorism missions. Over the past two decades, US SOF have deployed to remote and austere locations, operating with regional partners, providing resources, training, technology, and conducting operations that reduce the signature and attribution of the United States military. In the hybrid warfare context, these efforts have primarily involved the DoD and a few other government agencies, as the action arm overseas, with support from the DoS and interagency at large. This organizational framework and relationships within the current context could transition to focus on great power competition.

Deloitte's research on the future of SOF came to a similar conclusion—use SOF to counter hybrid warfare threats. The Deloitte study concluded, "SOF should be given the mandate and organic ability to plan and execute joint interagency operations and have a direct link to the national-level decision-makers. To accommodate hybrid warfare's requirements for speed, security, and coordination, the future SOF organization should operate dedicated, networked teams for interagency coordination and collaboration."[98] Deloitte is describing the construct of a JIATF. Assigning the lead to SOCOM, with other governmental agencies aligned in mutually supportive roles, could animate modest but effective hybrid and information warfare operations.

4. Enhance Public-Private cooperation and collaboration

Technology advances at exponential rates, requiring greater coordination with national research institutions, as well as the private sector, to build new capabilities for today's fight. In constructing JIATFs, the United States should look outside traditional skill sets to create diverse

[98] Taft, *Special Operations Forces and Great Power Competition*.

teams that resemble—not only a whole-of-government—but a whole-of-society. Take the Lower Manhattan Security Initiative, for example. This was a partnership between the New York Police Department (NYPD), Microsoft, and Manhattan banks to build a surveillance system after 9/11, known as the Domain Awareness System.[99] It allows the NYPD to track surveillance targets and gain detailed information about them. NYPD officers can use this data to inform decision making with analytics and operations research. Additionally, it gives them near real-time data to emerging threats in the city, enabling a more proactive and timely response to mitigate potential risks. Illustrating an example of a whole-of-society approach to counter a complex threat.

The skill sets and capabilities of a JIATF also need revision—from acquiring people with deep cultural experience in conflict areas of interest, to people with PhDs in artificial intelligence, data scientists and software engineers. These teams should also incorporate economists and social psychologists who are critical to support psychographic analysis and drafting a plan to condition behaviors towards the stated objectives. These teams need media experts, from journalists to social media influencers. In many ways, the skills and knowledge required are not traditional military occupational specialties, but skills that primarily reside in the civilian populace. In closing, World War II illustrated to the world what harnessing the United States private sector can do for a war effort. It required shifts in policy and new organizational frameworks to pull a whole-of-society effort together to defeat adversaries across all domains of conflict.

[99] Wikipedia search for *Domain Awareness System.* Retrieved from https://en.wikipedia.org/wiki/Domain_Awareness_System.

Conclusion

One of Secretary of Defense Forrestal's earliest memos to the National Security Council in 1948 urged "that our foreign information activities be effectively developed and that they be coordinated with the other phases of our foreign and military policies."[100] As it was during and following World War II, a whole-of-society approach is still very much needed today. However, hybrid warfare and leveraging the information instrument of national power is a lost art within the DoD, and in large part, the collective interagency. Seth Jones paints the picture quite clearly:

> "the United States largely abandoned these capabilities following the collapse of the Soviet Union. After 9/11, the United States focused on lethal, not political or information, operations: finding and targeting terrorists and other adversaries around the world with sophisticated intelligence and precision-strike capabilities. Yet these lethal capabilities are of limited value against adversaries who are fighting primarily with information and disinformation."[101]

To harness the full spectrum of United States national powers will require the level of collaboration, coordination, and integration across governmental agencies, and even the private sector, that followed 9/11.To paraphrase Frank Steder in his CTX article, the hybrid approach, when viewed through the lens of Prussian strategist Carl von Clausewitz and Chinese strategist Sun Tzu, as simply, warfare that uses all means necessary to achieve victory.[102]

---

[100] Inboden, William. Reforming American Power: Civilian National Security Institutions in the Early Cold War and Beyond (2016) in *Sustainable Security: Rethinking American National Security Strategy*. Oxford University Press, 149.

[101] Jones, Seth. *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare,* (Center for Strategic and International Studies, October 1, 2018). Retrieved from https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

[102] The Book of War: Sun Tzu, The Art of Warfare, & Karl von Clausewitz, On War (New York: Penguin Random House, 2000).

It took the collapse of the Twin Towers to make the necessary structural changes in the United States government—after only 19 terrorists found the seams to exploit vulnerabilities in an open and free society. It is the same vulnerabilities that great power competition attempts to disrupt. Policy and organizational changes lagged until it was too late, and then fundamentally changed the United States national security structure—hyper focused on the Global War on Terror. A new threat is clear and present, and so the United States should not wait for another tower to collapse, an election to be meddled with, or facts of a pandemic to be revised, before implementing the necessary changes to begin countering these asymmetric threats.

The research throughout this paper tells a very complex story, and the extreme efforts United States adversaries will attempt to shift global power. It is also a fresh reminder that war is fundamentally and primarily a human endeavor, and it is in the interest of all, that every effort be made to subdue the enemy before fighting. Due to the changing nature of conflict and advances in information technologies, shifts in authorities and foreign policies are required to align the intelligence community, United States government departments and agencies, and even the private sector in a more effective way. Conducting hybrid warfare and shaping the information environment are the new norms that the United States must contend with to prevent needless war and continue to lead the global liberal order. Even the current Chairmen of the Joint Chiefs of Staff, Army General Mark Milley, recognizes the need for the United States to improve its non-kinetic capabilities.[103] There have been too many conferences and discussion panels on admiring the problem—it is time to move past discussions and start organizing.

[103] Pomerleau, M. *Joint Chiefs nominee wants to boost information warfare*, (C4ISR Net, July 11, 2019). Retrieved from https://www.c4isrnet.com/information-warfare/2019/07/11/joint-chiefs-nominee-wants-to-boost-information-warfare/.

References

Bibliography

Avramov, Kiril and Ruslan Trad. *An experimental playground: The footprint of Russian private military companies in Syria*, (The Defense Post, February 17, 2018) Retrieved from https://thedefensepost.com/2018/02/17/russia-private-military-contractors-syria/.

Bartles, Charles. *Getting Gerasimov Right,* (Military Review, January-February 2016). Retrieved from https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/194973.

Bernd Horn, J. Paul de B. Taillon, and David Last, Force of Choice: Perspectives on Special Operations (Montreal: McGill-Queen's University Press, 2004).

The Book of War: Sun Tzu, The Art of Warfare, & Karl von Clausewitz, On War (New York: Penguin Random House, 2000)

Due-Gundersen, Nicolai. *Putin's Mercenaries Are Using Syria as a Training Ground*, (Lobe Log, August 20, 2019). Retrieved from https://lobelog.com/putins-mercenaries-are-using-syria-as-a-training-ground/.

Gan, Nectar, Caitlin Hu and Ivan Watson. *Beijing tightens grip over coronavirus research, amid US-China row on virus origin,* (CNN, April 13, 2020). Retrieved from https://www.cnn.com/2020/04/12/asia/china-coronavirus-research-restrictions-intl-hnk/index.html?utm_term=15867740039112da675e3714f&utm_source=Five+Things+for+Monday%2C+April+13+2020&utm_medium=email&utm_campaign=197814_1586774003917&bt_ee=7duN7Y0HOV7TpCOR%2Fbq6enmoFq0G90rKIbZYMuyBMw1cTqSCewmNfo9KiZJqGLMN&bt_ts=1586774003917.

Hsiao, Russell. *War Without Gunfire: China's Intelligence War with Taiwan,* (The Jamestown Foundation, November 5, 2010). Retrieved from https://jamestown.org/wp-content/uploads/2010/11/cb_010_239049.pdf?x12088.

Kramer, A. *Russian General Pitches 'Information' Operations as a Form of War,* (The New York Times, March 2, 2019). Retrieved from https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.

Mattis, Peter. *China's 'Three Warfares' In Perspective*, (War on the Rocks, January 30, 2018). Retrieved from https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

Mattis, Peter. *Contrasting China's and Russia's Influence Operations,* (War on the Rocks, January 16, 2018). Retrieved from https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations/.

Mattis, Peter and Alex Joske. *The Third Magic Weapon: Reforming China's United Front,* (War on the Rocks, June 24, 2019). Retrieved from https://warontherocks.com/2019/06/the-third-magic-weapon-reforming-chinas-united-front/.

McFate, S., *The Return of Mercenaries, Non-State Conflict, and More Predictions for the Future of Warfare*. (Go Medium Publication, Jan 22, 2019). Retrieved from: https://gen.medium.com/the-return-of-mercenaries-non-state-conflict-and-more- predictions-for-the-future-of-warfare-7449241a04e5.

Myers, Steven Lee. *China Spins Tale That the U.S. Army Started the Coronavirus Epidemic,* (The New York Times, March 17, 2020). Retrieved from https://www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html.

Owen, Jonathan. *British Army ramps up information warfare capability to meet 21st-century threats,* (PR Week, August 6, 2019). Retrieved from https://www.prweek.com/article/1593186/british-army-ramps-information-warfare-capability-meet-21st-century-threats.

Pomerleau, M. *Joint Chiefs nominee wants to boost information warfare,* (C4ISR Net, July 11, 2019). Retrieved from https://www.c4isrnet.com/information-warfare/2019/07/11/joint-chiefs-nominee-wants-to-boost-information-warfare/.

Raska, Michael. *Hybrid Warfare with Chinese Characteristics,* (ETHZurich, January 20, 2016). Retrieved from https://css.ethz.ch/en/services/digital-library/articles/article.html/195268/pdf.

Sussman, Bruce. *Make It a Dozen: New Lit of Hacker Names Russia Is Using in Cyber Attacks,* (Seguro Group Inc, October 4, 2018). Retrieved from https://www.secureworldexpo.com/industry-news/russia-government-hacker-names.

Taft, John, Liz Gormisky and Joe Mariani. *Special Operations Forces and Great Power Competition,*(Deloitte, June 17, 2019). Retrieved from https://www2.deloitte.com/uk/en/insights/industry/public-sector/future-of-special-operations-forces-great-power-competition.html.

Tagliabue, John. *Big Solidarity Victory Seen in Poland,* (The New York Times, June 5, 1989). Retrieved from https://www.nytimes.com/1989/06/05/world/big-solidarity-victory-seen-in-poland.html.

Tse-tung, Mao. *On Correcting Mistaken Ideas in the Party,* (Maoist Documentation Project, 2004). Retrieved from https://www.marxists.org/reference/archive/mao/selected-works/volume-1/mswv1_5.htm.

Veron, Emmanuel and Emmanuel Lincot. *Debate: How Beijing is trying to save face in the global fight against Covid-19,* (The Conversation, April 2, 2020). Retrieved from https://theconversation.com/debate-how-beijing-is-trying-to-save-face-in-the-global-fight-against-covid-19-134996.

Walton, Timothy. *China's Three Warfares,* (Delex Systems Inc., January 18, 2012). Retrieved from https://www.indianstrategicknowledgeonline.com/web/Three%20Warfares.pdf.

Wikipedia search for *Domain Awareness System.* Retrieved from https://en.wikipedia.org/wiki/Domain_Awareness_System.

Wong, Edward. *How China Uses LinkedIn to Recruit Spies Abroad.,* (The New York Times, September 27, 2019). Retrieved from https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.

Government Publications, Academic Journals, Think Tanks

2017 National Security Strategy of the United States of America, (The White House, December 2017). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

2018 National Defense Strategy Summary, (The Department of Defense, 2018). Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Berg-Knutsen, Espen. *From Tactical Champions to Grand Strategy Enablers: The Future of Small-Nation SOF in Counter-Hybrid Warfare,* (Combating Terrorism Exchange, November 2016). Retrieved from https://globalecco.org/documents/327413/327631/Vol+6+No+4.pdf/.

Center for Complex Operations Institute for National Strategic Studies. (2013). Convergence: Illicit Networks and National Security in the Age of Globalization. Washington D.C.: National Defense University Press.

Chinese National People's Congress Network. National Intelligence Law of the People's Republic, (June 27, 2017). Retrieved from http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

Chodkowski, W. M. *The United States Information Agency Fact Sheet*, (2012). Retrieved from https://www.americansecurityproject.org/ASP%20Reports/Ref%200097%20-%20The%20United%20States%20Information%20Agency.pdf.

Clements Center for National Security. *Russian Active Measures and the U.S. Response: Lessons from the Cold War*, (Clements Center, April 23, 2019). Retrieved from https://www.clementscenter.org/events/item/1633-a-conversation-with-seth-jones.

Cormac, Rory and Richard Aldrich. *Grey is the New Black: Covert Action and Implausible Deniability*, (International Affairs, May 2018). Retrieved from https://academic.oup.com/ia/article/94/3/477/4992414.

Crane, Conrad. *The U.S. Needs and Information Warfare Command: A Historical Examination,* (Information Professionals Association, June 14, 2019). Retrieved from https://information-professionals.org/the-u-s-needs-an-information-warfare-command-a-historical-examination/.

Department of State Bureau of Democracy, Human Rights, and Labor. *2019 Country Reports on Human Rights Practices: Taiwan,* (Department of State, 2019). Retrieved from https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/taiwan/.

Flynn, Michael Major General (Retired), Captain Matt Pottinger, Paul Batchelor. *Fixing Intel. A Blueprint for Making Intelligence Relevant in Afghanistan,* (Center for a New American Security, January 2010). Retrieved from https://online.wsj.com/public/resources/documents/AfghanistanMGFlynn_Jan2010.pdf, pg. 23.

Hoffman, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars,* (Potomac Institute for Policy Studies, December 2007). Retrieved from https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Inboden, William. Reforming American Power: Civilian National Security Institutions in the Early Cold War and Beyond (2016) in *Sustainable Security: Rethinking American National Security Strategy*. Oxford University Press.

Johnson, Scott. *Toward a Functional Model of Information Warfare*, (Center for the Study of Intelligence, April 14, 2007). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html.

Joint Concept for Human Aspects of Military Operations, (Joint Chiefs of Staff, October 19, 2016). Retrieved from https://nsiteam.com/social/wp-content/uploads/2017/01/20161019-Joint-Concept-for-Human-Aspects-of-Military-Operations-Signed-by-VCJCS.pdf.

Joint Interagency Task Force publication, (The Lightning Press, 2020). Retrieved from https://www.thelightningpress.com/joint-interagency-task-force-jiatf/.

Johnson, Oscar and Robert Seely. *Russian Full-Spectrum Conflict: An Appraisal After Ukraine*, (The Journal of Slavic Military Studies, Volume 28 2015). Retrieved from https://www.tandfonline.com/doi/abs/10.1080/13518046.2015.998118.

Jones, Seth. *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare*, (Center for Strategic and International Studies, October 1, 2018). Retrieved from https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

Kasapoglu, Can. *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*, (NATO Defense College Rome, November 2015). *Retrieved* from https://www.files.ethz.ch/isn/195099/rp_121.pdf.

Maizland, Lindsay and Andrew Chatzky. *Huawei: China's Controversial Tech Giant,* (Council on Foreign Relations, February 12, 2020). Retrieved from https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

Meredith III, Spencer Dr. *Countering Russian Strategic Approaches: Special Operations in Hybrid Warfare*, (National Defense University, 2019). Retrieved from https://nsiteam.com/social/wp-content/uploads/2019/06/Countering-Russian-Strategic-Approaches-SMA-JUN-2019-SBM-converted.pdf.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019.* Retrieved from https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

National Intelligence Estimate. *Soviet Goals and Expectations in the Global Power Arena*, (Central Intelligence Agency, July 7, 1981). Retrieved from https://www.cia.gov/library/readingroom/docs/DOC_0000268220.pdf.

Robinson, L. Helmus, T. Cohen, R. Nader, A. Radin, A. Magnuson, M. Migacheva, K. *Modern Political Warfare: Current Practices and Possible Responses*. (RAND Corporation, 2018). 15.

Steder, Frank. *Introduction, The Theory, History and Current State of Hybrid Warfare*, (Combating Terrorism Exchange, November 2016). Retrieved from https://globalecco.org/documents/327413/327631/Vol+6+No+4.pdf/.

Vergun, David. *DOD Comptroller: Overmatch Against China, Russia* Critical, (U.S. Department of Defense, April 10, 2019). Retrieved from https://www.defense.gov/Explore/News/Article/Article/1810790/dod-comptroller-overmatch-against-china-russia-critical/.

Votel, Joseph , Charles Cleveland, Charles Connett and Will Irwin. *Unconventional Warfare in the Gray Zone*, Joint Force Quarterly 80, (National Defense University Press, January 2016). Retrieved from https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/.

Interviews

Avramov, Kiril. (2020, January 31). Personal Interview.

Brooks, Vincent General (Retired). (2020, February 10). Personal Interview.

Buchanan, Jeffrey Lieutenant General (Retired). (2020, February 15). Personal Interview.

Reeder, Ed Major General (Retired). (2020, February 10). Personal Interview.