JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

Vol. 12, No. 1, 2021

JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

MCUP

Published by Marine Corps University Press
2044 Broadway Street | Quantico, VA 22134

Journal of Advanced Military Studies
(Print) ISSN 2164-4209
(Online) ISSN 2164-4217

DISCLAIMER

The views expressed in the articles and reviews in this journal are solely those of the authors. They do not necessarily reflect the opinions of the organizations for which they work, Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government. When necessary, errata will be published immediately following the book reviews.

FREELY AVAILABLE AT
www.usmcu.edu/mcupress

Established in 2008, MCU Press is an open access publisher that recognizes the importance of an open dialogue between scholars, policy makers, analysts, and military leaders and of crossing civilian-military boundaries to advance knowledge and solve problems. To that end, MCUP launched the *Journal of Advanced Military Studies* (JAMS) to provide a forum for interdisciplinary discussion of national security and international relations issues and how they have an impact on the Department of Defense, the Department of the Navy, and the U.S. Marine Corps directly and indirectly. JAMS is published biannually, with occasional special issues that highlight key topics of interest.

ARTICLE SUBMISSIONS

The editors are looking for academic articles in the areas of international relations, geopolitical issues, national security and policy, and cybersecurity. To submit an article or to learn more about our submission guidelines, please email MCU_Press@usmcu.edu.

BOOK REVIEWS

Send an email with a brief description of your interests to MCU_Press@usmcu.edu.

SUBSCRIPTIONS

Subscriptions to JAMS are free. To join our subscription list or to obtain back issues of the journal, send your mailing address to MCU_Press@usmcu.edu.

ADDRESS CHANGE

Send address updates to MCU_Press@usmcu.edu to maintain uninterrupted delivery.

INDEXING

The journal is indexed by EBSCO, ProQuest, OCLC ArticleFirst, Defense Technical Information Center (DTIC), JournalSeek, IBZ Online, British Library System, Lancaster Index to Defense and International Security Literature, and AU Library Index to Military Periodicals.

The production of this journal and other MCUP products is graciously supported by the Marine Corps University Foundation.

Contents

Vol. 12, No. 1

POLITICAL WARFARE AND PROPAGANDA

REVIEW ESSAYS

BOOK REVIEWS

Call for Submissions

Marine Corps University Press (MCUP) offers a variety of scholarly publishing opportunities for faculty, staff, and advanced graduate-level students. In addition to a full catalog of monographs covering Marine Corps history and national security/international relations topics, MCUP also publishes three journals.

Expeditions with MCUP

Expeditions with MCUP, an online academic journal, offers authors a forum for the debate of trending domestic and international topics. Articles cover topics ranging from national security, international relations, political science, and geopolitics as they apply to and impact the Department of Defense, Department of the Navy, and Marine Corps. Submissions accepted throughout the year.

Marine Corps History (MCH)

MCUP publishes MCH twice a year on all topics within the long history of the Corps: Civil War, Spanish-American War, Banana Wars, WWI, WWII, Korea, Cold War, Vietnam, Iraq, Afghanistan, and women and minorities in the Marines. Articles must focus on some aspect of the Corps, either directly or indirectly, including foreign marines and Joint operations. Submissions accepted by January (summer issue) or July (winter issue).

Journal of Advanced Military Studies (JAMS)

The *Journal of Advanced Military Studies* (JAMS) focuses on topics of concern to the Marine Corps and the Department of Defense through the lens of various disciplines, including international relations, political science, security studies, and political economics. Articles may discuss topics from a historical, contemporary, or forward-looking perspective. The Fall 2021 issue will focus on the past, present, and future state of wargaming and the military. Submissions due by 31 July 2021. The Spring 2022 issue of JAMS will focus on how militaries respond to national emergencies and natural disasters. Submissions due by 1 January 2022.

Article submissions for all three journals should be between 4,000 and 10,000 words, footnoted, and formatted according to the *Chicago Manual of Style* (17th edition). For submission guidelines or to submit an article idea, please visit our website or contact MCU_Press@usmcu.edu.

www.usmcu.edu/mcupress

From the Editors

In early 2020, when the editors and the Marine Corps University Press editorial board were planning for the 2021 *Journal of Advanced Military Studies* (JAMS) publishing schedule, we could not have predicted the events that would unfold during that time—a global pandemic killing thousands of people per day, massive unemployment, voter fraud conspiracy theories, and a seditious attack on the U.S. Capitol. We can only point to the fortuitous nature of publishing that we are able to bring you this issue of JAMS on information warfare and propaganda at a time when readers need reliable information most.

The events of 2020–21 are neither the first examples of information warfare and propaganda nor will they be the last. The Trojan horse of Homer's *The Odyssey* stands as one of the most well-known examples of classical information warfare in literature, but military history is filled with nonfiction instances as well. Sun Tzu believed that "all warfare is deception," and therefore warfare is based on the use or misuse of information as well as military force.[1]

What is the difference between information warfare then and now? Further, how does it differ from the term *propaganda*? One early definition refers to *information warfare* as

> any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions.[2]

A conference of analysts discussing intelligence reform at Stanford University would later define information warfare as

> a struggle over the information and communications process, a struggle that began with the advent of human communication and conflict. . . . Information warfare is the application of destructive force on a large scale against information assets and systems, against the computers and networks that support the

> four critical infrastructures (the power grid, communications, financial, and transportation).[3]

In more contemporary terms, the North Atlantic Treaty Organization (NATO) defines information warfare as

> an operation conducted in order to gain an information advantage over the opponent. It consists in controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. Information warfare is not a new phenomenon, yet it contains innovative elements as the effect of technological development, which results in information being disseminated faster and on a larger scale.[4]

If information warfare focuses on concepts of advantage, destruction, and acquisition, then how does propaganda differ? For the purposes of this discussion, we will refer to propaganda as the dissemination of information—facts or lies—to influence public opinion. However, the reader is cautioned to remember that the deliberate emphasis on *manipulation* distinguishes propaganda from what many might consider casual conversation or the free exchange of ideas.

If we consider NATO's approach to information warfare, the activities within this spectrum present as significantly more militant, even combative, characteristics, particularly if they have the ability to impact U.S. national security objectives as they have during operations in the Middle East and Europe. As information warfare continues to evolve in the face of technological disruptions that outpace a country's ability to defend against it, the United States must be strategically placed to protect against and attack those who might use information warfare, propaganda, and disinformation campaigns to their advantage on the battlefield, inside the voting booth, or throughout media and social media.[5]

The authors for this issue of JAMS did not back down from the often-controversial nature of this topic as they present multiple perspectives on past events, current issues, and possible ways forward for the country. The first article by Daniel de Wit offers a historical case study of the Office of Strategic Services (predecessor of the modern Central Intelligence Agency) and the psychological warfare and resistance operations in World War II.

As we transition from the early twentieth century to modern issues, James Forest provides an introductory article that prefaces the political warfare and propaganda concepts presented by the remaining articles, including a brief examination of terms, concepts, and examples of these efforts.

Dr. Kyleanne Hunter and Emma Jouenne discuss gender integration and the impact of misogyny and racial social media propaganda on enlistment and service. The authors' case studies—the United States Military, the involuntary celibate (incel) movement, and the Islamic State in Iraq and Syria (ISIS)—demonstrate that "while the Internet and social media have allowed for advancements in communication, economics and education, it has also emboldened and elevated vitriolic forms of misogyny." The authors hypothesize that online misogyny negatively impacts military recruiting and intensifies the violent tendencies of radical groups.

Dr. Glen Segell's article, "Consistency of Civil-Military Relations in the Israel Defense Forces: The Defensive Mode in Cyber," considers how the IDF may be engaged in a total war but must do so in a defensive mode; and yet they are also involved in a limited war in the offensive mode as their adversaries do not share the same policies regarding cyber and terror attacks against civilian, government, and military targets.

Drs. Lev Topor and Alexander Tabachnik move the discussion from Israel to Russia's use of cyber information warfare as a tool for international distribution and domestic control. The authors consider how nation-states see significant impacts to their national security as a result of information warfare, yet Russia has managed to wield it as a weapon so effectively against its adversaries while also protecting itself from external information warfare. Russia relies on "uncompromising control over its domestic cyberspace, thus restricting undesirable informational influence over its population."

Donald M. Bishop continues this thread with his article, "Propagandized Adversary Populations in a War of Ideas." He argues that "the internet, social media, and the cell phone have transformed the channels of propaganda, but in the twenty-first century, a few adversaries—China, North Korea, Russia, Iran, Cuba, and Venezuela—still draw on the experience of the twentieth century. They control the information that circulates in their societies, and they deploy domestic and international propaganda to strengthen their exercise of national power." As the U.S. military, and the Marine Corps in particular, position themselves for great power competition, they must consider the role of propaganda in this battle and what tools should be implemented in our defense.

Colonel Phil Zeman pushes the power competition debate to the next level with his concept of social antiaccess/area-denial (A2/AD). Zeman believes that "this threat is subtle and coercive in nature, targeting not the military or government but industry and citizens. It is designed to exploit social dynamics and economic propensities by creating dependencies on foreign capacities."

Further, our adversaries are already entrenched in this battlespace, which leaves the United States to race to defend what our adversaries have enabled to become so pervasive in our society.

Dr. Michael Cserkits's article, "Representation of Armed Forces through Cinematic and Animated Pieces: Case Studies," examines the representation of armed forces in cinematic productions and anime to shed light on the societal representation of but also the desired self-identification and goals of the armed forces using the United States and Japan as case studies. The desired goal of both is to gain support and backup for their servicemembers, regardless of their tasks or missions.

Our final article, "Streaming the Battlefield: The Internet's Effect on Negotiation Onset," by First Lieutenant Anthony Patrick offers some potential closure to this conversation as he considers how all the previous concepts—information warfare, propaganda, technology, etc.—impact a nation's ability to negotiate during times of conflict. Based on Patrick's research, "the bargaining model of war breaks down once you move into conflicts where parties do not have some level of parity. Without near parity there is no true incentive for the powerful party to enter negotiations with the significantly weaker power."

The remainder of the journal rounds out with a selection of review essays and book reviews that continues our focus on information warfare and propaganda, but it also highlights continuing challenges in national security and international relations. The coming year will be busy for the JAMS editors as we work to provide journal issues on a diverse range of topics relevant to the study of militaries and defense.

The upcoming Fall 2021 issue of JAMS encourages authors to consider the past, present, and future state of wargaming and the military. The editors are also interested in acquiring content for a special issue of JAMS that focuses on strategic culture. The Spring 2022 issue of JAMS will open a larger discussion of the historic, contemporary, and future roles of military Services during national emergencies and natural disasters. Contribute to the discussion and submit an article for consideration. We look forward to hearing your thoughts on these topics and to your future participation as an author, reviewer, or reader.

Join the conversation and find us online on our LinkedIn page (https://tinyurl.com/y38oxnp5), at MC UPress on Facebook, MC_UPress on Twitter, and MCUPress on Instagram or via email at MCU_Press@usmcu.edu.

Endnotes

1. Robert R. Mackey, "Information Warfare," *Oxford Bibliographies* (March 2014), https://doi.org/10.1093/OBO/9780199791279-0024.
2. Gen Ronald R. Fogelman (USAF) and Sheila E. Widnall, *Cornerstones of Information Warfare* (Washington, DC: U.S. Air Force, 1997).

3. Brian C. Lewis, "Information Warfare," in *The Final Report of the Snyder Commission*, ed. Edward Cheng and Diane C. Snyder (Princeton, NJ: Woodrow Wilson School of Public and International Affairs, Princeton University, 1997).
4. "Media—(Dis)information—Security," NATO, May 2020.
5. For more on how these activities might impact the Services, the Marine Corps in particular, see Miriam Matthews et al., *Frameworks for Assessing USEUCOM Efforts to Inform, Influence, and Persuade* (Santa Monica, CA: Rand, 2020), https://doi.org/10.7249/RR2998; and Michael Schwille et al., *Improving Intelligence Support for Operations in the Information Environment* (Santa Monica, CA: Rand, 2020), https://doi.org/10.7249/RB10134.

Political Warfare and Propaganda
An Introduction

James J. F. Forest, PhD

Abstract: The digital age has greatly expanded the terrain and opportunities for a range of foreign influence efforts. A growing number of countries have invested significantly in their capabilities to disseminate online propaganda and disinformation worldwide, while simultaneously establishing information dominance at home. This introductory essay provides a brief examination of terms, concepts, and examples of these efforts and concludes by reviewing how the articles of this issue of the *Journal of Advanced Military Studies* contribute to our understanding of political warfare and propaganda.

Keywords: information operations, digital influence, political warfare, psychological warfare

In 1970, Canadian media theorist Marshall McLuhan predicted that World War III would involve "a guerrilla information war with no division between military and civilian participation."[1] More than 30 years later, in their 2001 groundbreaking book *Networks and Netwars: The Future of Terror, Crime, and Militancy*, John Arquilla and David Ronfeld described how

> the conduct and outcome of conflicts increasingly depend on information and communications. More than ever before, conflicts revolve around "knowledge" and the use of "soft power." Adversaries are learning to emphasize "information operations" and "perception management"—that is, media-

James J. F. Forest is a professor at the School of Criminology & Justice Studies, University of Massachusetts Lowell and a visiting professor at the Fletcher School, Tufts University. He has published more than 20 books in the field of international security studies, most recently *Digital Influence Warfare in the Age of Social Media* (2021) and *Digital Influence Mercenaries* (2021).

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201001

> oriented measures that aim to attract or disorient rather than coerce, and that affect how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries. Psychological disruption may become as important a goal as physical destruction.[2]

How prescient these observations seem today, particularly given how malicious actors—both foreign and domestic—are now weaponizing information for the purpose of influencing political, economic, social, and other kinds of behavior.

This issue of the *Journal of Advanced Military Studies* addresses the intersection of political warfare and the digital ecosystem. To frame the contributions that follow, this introduction to the issue reviews the broad landscape of terms and concepts that refer to the weaponization of information, and then provides a small handful of historical and modern examples that reflect the goals and objectives pursued through influence efforts. The discussion then turns to describe how the articles in this issue contribute to our understanding of political warfare and propaganda in the digital age, before concluding with some thoughts about the need for research-based strategies and policies that can improve our ability to defend against foreign influence efforts and mitigate their consequences.

A Diverse Landscape of Terms and Concepts

The past several centuries have largely been defined by physical security threats, requiring a nation's military to physically respond with whatever means they have available. But as explained by Isaiah Wilson III—president of Joint Special Operations University—today we face "compound security threats," which include physical security threats as well as "communication and information operations that scale with the speed of a social media post that goes viral, as well as cyber warfare, hacking and theft by our adversaries, both state and non-state actors."[3] These compound security threats can exploit cybersecurity vulnerabilities as well as psychological and emotional vulnerabilities of targets, using modern internet platforms to reach targets worldwide.

Terms like *information operations* or *information warfare* have been frequently used in military doctrine to describe computer network attacks (often by highly trained military units) like hacking into databases to observe or steal information, disrupting and degrading a target's technological capabilities, weakening military readiness, extorting financial ransoms, and much more. These terms have also referred to operations intended to protect our own data from these attacks by adversaries. Computer network attacks like these can also be used to send a message (e.g., about a target's vulnerabilities and the attacker's capabilities), and in that way could be a means of influencing others. Cyberattacks are seen as compound security threats because they can have implications for multiple dimensions of a nation's well-being, including politics, economics, technology, information security, relations with other countries, and much more.

Today's digital influence attacks also have implications for these same multiple dimensions and are likewise seen as compound security threats. The goals of digital influence attacks can include disrupting and degrading a target's societal cohesion, undermining confidence in political systems and institutions (i.e., democratic elections), fracturing international alliances, and much more. Tactics used in such attacks include various forms of deception and provocation, from deepfake videos and fake social media accounts to gaslighting, doxing, trolling, and many others. Through social media and other internet technologies, attackers can incentivize and manipulate interactions directly with citizens of a foreign population, bypassing government efforts to insulate their citizens from an onslaught of disinformation.[4] These types of attacks exploit human vulnerabilities more than technological attacks and capitalize on psychological and emotional dimensions like fear, uncertainty, cognitive biases, and others.

A variety of terms are used to describe these attacks, sometimes leading to confusion rather than clarity. The term *political warfare* was used by the legendary diplomat George Kennan in 1948 to describe "the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert and can include various kinds of propaganda as well as covert operations that provide clandestine support to underground resistance in hostile states."[5] Paul A. Smith describes political warfare as "the use of political means to compel an opponent to do one's will" and "its chief aspect is the use of words, images, and ideas, commonly known, according to context, as propaganda and psychological warfare."[6] Carnes Lord notes a "tendency to use the terms psychological warfare and political warfare interchangeably" along with "a variety of similar terms—ideological warfare, the war of ideas, political communication and more."[7] And the U.S. Department of Defense has used the term *military information support operations* to describe efforts to "convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."[8]

In a 2019 research report published by Princeton University, Diego A. Martin and Jacob N. Shapiro illustrate how "foreign actors have used social media to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation."[9] The researchers define *foreign-influence efforts* as: 1) coordinated campaigns by one state to impact one or more specific aspects of politics in another state, 2) through media channels, including social media, and by 3) producing content designed to appear indigenous to the target state.[10] The objective of such campaigns can be quite broad and to date have included influencing political decisions by shaping election outcomes at various levels, shifting the political agenda on topics ranging from health to security, and encouraging political polarization.[11] Similarly, research by Philip N. Howard describes "countries with dedicated teams meddling in the affairs of their neighbors through social media misinformation."[12] And social media platforms—most notably Facebook—are now using the term *information operations* when referring to deliberate and systematic attempts to steer public opinion using inauthentic accounts and inaccurate information.[13]

A recent book by Carl Miller describes how "digital warfare has broken out between states struggling for control over what people see and believe."[14] Other terms used in the literature include "new generation warfare," "ambiguous warfare," "full-spectrum warfare," and "non-linear war."[15] Scholars have also described these security challenges as forms of hybrid warfare, encompassing a combination of political warfare, psychological operations, and information operations (including propaganda). Similar terms in this broad landscape include *public diplomacy* and *strategic communications*. Further, some states are portrayed as pursuing "information dominance" over the populations of other states through a combination of computer network operations, deception, public affairs, public diplomacy, perception management, psychological operations, electronic countermeasures, jamming, and defense suppression.[16]

Whatever we want to call it, there are clear examples of aggression, attackers, targets, defenders, tactics, strategies, goals, winners, losers, and innocent victims. And this is not something that only states do to other states: non-state actors are increasingly engaged in these kinds of activities as well.[17] The author's own work has used the term *influence warfare* to describe the kinds of activities in which the focus is not the information but on the *purposes* of that information.[18] This conceptual approach views the implicit goal of spreading propaganda, misinformation, disinformation, and so forth as shaping perceptions and influencing behavior of a specific target (or set of targets). Further, influence warfare strategies and tactics—particularly as we have seen online—also involve more than just manipulation of information; they can include behavior signaling (e.g., swarming or bandwagoning), trolling, gaslighting, and other means by which the target is provoked into having an emotional response that typically overpowers any rational thought or behavior.[19] Clickbait, memes, and ragebait (for example) are not really seen as forms of information operations as traditionally conceived, but they are certainly ways of influencing others via the internet. This leads us to the term *digital influence warfare,* which will be used variably throughout this introduction as a catchall phrase representing the broadly diverse terrain of political and psychological warfare in the digital age.[20]

Strategic Goals and Tactics of Influence Warfare

The "weaponization of information" in order to obtain power and influence is of course not new. The principles of influence warfare are based on an ancient and much-repeated maxim, attributed to the Chinese general and military theorist Sun Tzu, paraphrased as "to win one hundred victories in one hundred battles is not the highest skill. To subdue the enemy without fighting is the highest skill."[21] When the thirteenth-century Mongols were rolling across Eurasia, they deliberately spread news of the atrocities they perpetrated on cities that did not surrender, the obvious goal being what Sun Tzu argued was the ultimate victory: to defeat the enemy before a single shot has been fired. As Marc Galeotti explains, fear is a powerful emotion, and in this instance it was used to coerce the behavior of cities the Mongols had in their sights, preferring that they surrender instead of having to spend valuable resources conquering them through force.[22] Mongol hordes would also drag branches behind their horses to raise dust clouds suggesting their armies were far larger than reality—an early and effective form of deception and disinformation.

The previous century saw a wide variety of efforts involving the weaponization of information for strategic purposes. During the Chinese Civil War (1945–49), both the Communist and Nationalist (Kuomintang, or KMT) armies spread false information to sow discord in enemy-controlled areas, spreading rumors about defections, falsifying enemy attack plans, and stirring up unrest in an effort to misdirect enemy planning. After the Nationalist government relocated to Taiwan in 1949, the influence efforts continued as the two sides flooded propaganda and disinformation into enemy-controlled territories to affect public opinion and troop morale.[23] Various forms of influence warfare also played a major role in both World Wars. For example, the Committee on Public Information was created during World War I by U.S. president Woodrow Wilson to facilitate communications and serve as a worldwide propaganda organization on behalf of the United States.[24]

Influence warfare was increasingly prominent throughout World War II, especially the massive amounts of propaganda disseminated by Joseph Goebbels and the Nazi regime. In response, U.S. president Franklin D. Roosevelt established the Office of War Information in 1942, responsible for (among other things) undermining the enemy's morale—often through various psychological and information operations—as well as for providing moral support and strengthening the resolve of resistance movements in enemy territories. The Voice of America (VOA) was also established in 1942 as the foreign radio and television broadcasting service of the U.S. government, broadcasting in English, French, and Italian. Years later, the United States Information Agency (USIA) was created in 1953 as a primary conduit for enhancing our nation's strategic influence during the Cold War.[25] The director of USIA reported to the president through the National Security Council and coordinated closely with the secretary of state on foreign policy matters.

Meanwhile, when Radio Moscow began broadcasting in 1922, it was initially available only in Moscow and its surrounding areas, but by 1929, the Soviets were able to broadcast into Europe, North and South America, Japan, and the Middle East using a variety of languages.[26] By 1941, the Union of Soviet Socialist Republics (USSR) was able to broadcast in 21 languages and, 10 years later, had a program schedule of 2,094 hours.[27] But radio and television broadcasting were just the visible tip of the iceberg for what became a multidimensional influence effort during the Cold War involving an array of covert influence tactics, particularly through the spread of disinformation. As Thomas Rid notes, "Entire bureaucracies were created in the Eastern bloc during the 1960s for the purpose of bending the facts."[28] The Soviets used disinformation "to exacerbate tensions and contradictions within the adversary's body politic, by leveraging facts, fakes, and ideally a disorienting mix of both."[29]

In the first academic study of the Soviet-era active measures program, Richard H. Shultz and Roy Godson explain how the Soviets cultivated several different types of so-called "agents of influence . . . including the unwitting but manipulated individual, the 'trusted contact,' and the controlled covert agent."[30] As they explain,

> The agent of influence may be a journalist, a government official, a labor leader, an academic, an opinion leader, an artist, or involved in a number of other professions. The main objective of an influence operation is the use of the agent's position—be it in government, politics, labor, journalism or some other field—to support and promote political conditions desired by the sponsoring foreign power.[31]

Forged documents—including faked photographs—have also been a part of influence warfare for more than a century. For example, during the 1920s the Soviet Cheka (secret police) used elaborate forgeries to lure anti-Bolsheviks out of hiding, and many were captured and killed as a result.[32] During the Cold War, as Shultz and Godson note, many "authentic-looking but false U.S. government documents and communiqués" could be categorized mainly as either "altered or distorted versions of actual US documents that the Soviets obtained (usually through espionage)" or "documents that [were] entirely fabricated."[33] Examples include falsified U.S. State Department documents ordering diplomatic missions to sabotage peace negotiations or other endeavors, fake documents outlining U.S. plans to manipulate the leaders of Third World countries, or even forged cables from an American embassy outlining a proposed plan to overthrow a country's leader.[34]

In one case, an authentic, unclassified U.S. government map was misrepresented as showing nuclear missiles targeting Austrian cities. A fabricated letter ostensibly written by the U.S. defense attaché in Rome contained language denying "rumors suggesting the death of children in Naples could be due to chemical or biological substances stored at American bases near Naples," while no such substances were stored at those bases.[35] Even a fake U.S. Army Field Manual was distributed, purportedly encouraging Army intelligence personnel to interfere in the affairs of host countries and subvert foreign government officials and military officers.[36] Through these and other types of information operations, the Soviets tried to influence a range of audiences, and the lessons to be learned from this history—both successes and failures—can inform the influence warfare efforts of many countries today.

Influence Opportunities in the Digital Age

While the primary strategies and goals of influence warfare have remained fairly constant, the operational environment in which these efforts take place has changed significantly during the past two decades. The rise of the internet and social media companies, whose profit model is based on an attention economy, has been a game changer. Within the attention economy, the most valued content is that which is most likely to attract attention and provoke engagement, with no regard to whether it is beneficial or harmful, true or untrue. New tools have emerged for creating and spreading information (and disinformation) on a global scale. Connectivity in the digital realm is now much easier, and yet the emergence of hyperpartisan echo chambers has sequestered many online users into separate communities who reject the credibility and merits of each other's ideas, beliefs, and narratives.

Unlike conventional cyberattacks, the goal of a digital influence warfare campaign is not about degrading the functional integrity of a computer system. Rather, it is to use those computer systems against the target in whatever ways might benefit that attacker's objectives. Often, those objectives include a basic divide and conquer strategy—a society that is disunited will fight among themselves over lots of things, instead of coming together in the face of a threat that only some of them believe is there. Many influence activities are meant to shape the perceptions, choices, and behaviors of a society—and in some cases, the goal may in fact be making the target dysfunctional as a society. This is not simply propaganda, fake news, or perception manipulation. It is a battle over what people believe is reality and the decisions that each individual makes based on those beliefs. The victors in this battle are the attackers who have convinced scores of victims to make decisions that directly benefit the attackers.

Digital influence warfare involves the use of persuasion tactics, information and disinformation, provocation, identity deception, computer network hacking, altered videos and images, cyberbullying, and many other types of activity explored in this issue of the *Journal of Advanced Military Studies*. The attacker (or "influencer") seeks to weaponize information against a target in order to gain the power needed to achieve the goals articulated in their strategic influence plan. Some goals may involve changing the target's beliefs and behaviors, prompting the targets to question their beliefs in the hopes that once those beliefs have been undermined, the targets may change their minds. Other goals may include manufacturing uncertainty to convince the target that nothing may be true and anything may be possible.[37] In other instances, the goals of an influence strategy could include strengthening the target's certainty, even their commitment to believing in things that are actually untrue.

The central goal of influence attacks is—according to a recent report by Rand—"to cause the target to behave in a manner favorable to the influencer."[38] The influencer may seek to disrupt the target's information environment—for example, interrupting the flow of information between sources and intended recipients of an organization, or on a broader level, between the target's government and its citizens. Similarly, the influencer may also seek to degrade the quality, efficiency, and effectiveness of the target's communication capabilities, which may involve flooding channels of communication with misinformation and disinformation. The overall goal here involves undermining the perceived credibility and reliability of information shared among the adversary's organizational members (government or corporate) or between the target's government and its citizens.[39] Attackers in the digital influence domain can organize swarms of automated social media accounts ("bots") alongside real accounts, coordinated to amplify a particular narrative or attack a specific target. Government (or corporate) leaders can hire technically skilled mercenaries and contractors (from large so-called social media influence corporations to lone hackers) to do the dirty work for them.[40]

Based on whatever goals the attacker wants to achieve, they will need to identify the targets they want to influence. When conducting research on their targets, the attackers will seek to answer specific questions like: What do they already believe about their world and/or their place within it? What do they think they know, and what are they uncertain about? What assumptions, suspicions, prejudices, and biases might they have? What challenges and grievances (economic, sociopolitical, security, identity, etc.) seem to provoke the most emotional reactions among them? Throughout the history of influence warfare, this information has been relatively easy to identify in open liberal democracies of the West. In more closed or oppressed societies, an additional step may be needed to determine how the target audience's perceptions compare to the discourse in the public domain—for example, what the news media (often owned and controlled by the government) identify as important topics and acceptable views within that society may not fully reflect the reality.

Influence efforts should always be guided by data on potential targets. An attacker should never waste their resources on target audiences that are already well-armed to repeal the influence efforts; better instead to identify vulnerable targets to exploit. For example, if the goal is to sow division and increase political polarization within a society, the United States offers a prime target for achieving that goal. Research by the Oxford Internet Institute in 2019 has found that people in the United States share more junk news (i.e., completely fabricated information disguised to look like authentic news) than people in other advanced democracies such as France, Germany, and the United Kingdom.[41] A study by the Pew Research Center in 2017 found that 67 percent of U.S. adults received news through social media sites like Twitter and Facebook.[42] Further, analysis of Russian influence efforts by the Atlantic Council's Digital Forensic Research Lab in 2018 found that Americans were vulnerable to a distinct type of troll accounts that used "carefully crafted personalities" to infiltrate activist communities and post hyperpartisan messages in order to "make their audiences ever more radical."[43]

These research studies reflect another important dimension of influence efforts: after gathering enough quality information about the target, the attacker will then seek to establish a foothold in the information environment preferred by that target. They must establish a credible presence among an audience of like-minded social media users before attempting to influence or polarize that audience. A common approach involves initially posting some messages that the target audience is likely to agree with. The convention of "like" or "share" facilitated by social media platforms can draw the target toward recognition of an acceptable persona (the "like-minded, fellow traveler").[44] Once established within the target's digital ecosystem, the persona can then begin to shape perceptions and behavior in ways that will benefit their influence strategy.

Perhaps the most well-known example of this in the public arena today is called disinformation or fake news. Essentially, these are forms of information deception, and there are several variations to consider. According to researcher Claire Wardle, some of the most "problematic content within our information ecosystem" includes:

- False connection: when headlines, visuals, or captions do not support the substance or content of the story itself;

- Misleading content: misleading use of information to frame an issue or individual;
- False context: when genuine content is shared with false contextual information;
- Imposter content: when genuine sources are impersonated;
- Manipulated content: when genuine information or imagery is manipulated to deceive (altered videos and images, including deepfakes, are the most prevalent examples of this); and
- Fabricated content: new content is 100 percent false and designed to deceive and do harm.[45]

Each of these forms of "problematic content" has a role to play in achieving an influence warfare strategy. Further, in many cases the most effective means of using these types of information (or disinformation) involves a careful integration between fake details and accurate details that the target already accepts as true. In the field of education, teachers often refer to the concept of *scaffolding* as a strategy to foster learning by introducing material that builds on what the student already understands or believes. For the purposes of an influence strategy, as Thomas Rid explains, for disinformation to be successful it must "at least partially respond to reality, or at least accepted views."[46]

Additional examples of deceptive digital influence tactics include identity deception (e.g., using fake or hijacked social media accounts) and information source deception (e.g., rerouting internet traffic to different sources of information that seem legitimate but relays false information to the viewers). As with the other forms of deception, a primary intent of these tactics is for the influencer to make the target believe what is not true. Similarly, the influencer may also spread disinformation through the target's trusted communication channels to degrade the integrity of their decision making and even their perception of reality.

Of course, deception is only one of several digital influence strategies. Another, which we have seen in use frequently in recent years, is to encourage engagement—especially by provoking emotional responses—using information that may in fact be all or partially accurate. Unlike disinformation and deception, the primary focus here is less on the message than on provoking people to propagate the message. Effective targets for this approach are those who have higher uncertainty about what is true or not but are willing to share and retransmit information without knowing whether it is untrue (and often because they want it to be true). And it is widely understood that fear is an exceptionally powerful emotion that can lead people to make a wide variety of (often unwise) decisions.

There are many kinds of influence goals that can be achieved by intentionally provoking emotional responses, usually in reference to something that the target already favors or opposes. The tactic of provoking outrage can be particularly effective here against a target audience—as Sun Tzu wrote, "Use anger to throw them into disarray."[47] With the right sort of targeting, message format, and content, the influencer can use provocation tactics to produce whatever kinds of behavior they want by the target (e.g., angrily lashing out at members of an opposing political party or questioning the scientific evidence behind an inconvenient truth). And an additional type of influence warfare involves attacking the target directly—threatening or bullying them, calling them derogatory names, spreading embarrassing photos and videos of them, and so forth.

One of the most well-known earlier forms of digital influence warfare was North Korea's attack against Sony. In the summer of 2014, Sony Pictures had planned to release a comedy, *The Interview*, featuring a plot in which two bumbling, incompetent journalists score an interview with Kim Jong-un, but before they leave they are recruited by the Central Intelligence Agency (CIA) to blow him up.[48] An angered North Korea responded by hacking into Sony's computer networks, destroying some key systems and stealing tons of confidential emails that they later released publicly in small, increasingly embarrassing quantities. Details about contracts with Hollywood stars, medical records, salaries, and Social Security numbers were also released. But unlike other well-reported cyberattacks of that era, this was—in the words of David E. Sanger—"intended as a weapon of political coercion."[49] As with many other examples of this hack and release tactic, the strategic goals are fairly straightforward: for example, to weaken an adversary by undermining its perceived credibility. This same script was followed by Russia during the 2016 U.S. presidential election, when they hacked into John Podesta's email account and released (via WikiLeaks) a stream of embarrassing messages (as detailed in the investigation report by former Federal Bureau of Investigation [FBI] director Robert S. Mueller III).[50]

Today, states are engaged in these kinds of digital influence activities with increasing regularity and sophistication. As a July 2020 report by the Stanford Internet Observatory explains:

> Well-resourced countries have demonstrated sophisticated abilities to carry out influence operations in both traditional and social media ecosystems simultaneously. Russia, China, Iran, and a variety of other nation-states control media properties with significant audiences, often with reach far beyond their borders. They have also been implicated in social media company takedowns of accounts and pages that are manipulative either by virtue of the fake accounts and suspicious domains involved, or by way of coordinated distribution tactics

> to drive attention to certain content or to create the perception that a particular narrative is extremely popular.[51]

China in particular has significantly ramped up its digital foreign-influence efforts, to include disrupting Twitter conversations about the conflict in Tibet and meddling in Taiwanese politics.[52] In fact, public opinion warfare and psychological warfare are closely intertwined in Chinese military doctrine. According to a recent Pentagon report, China's approach to psychological warfare "seeks to influence and/or disrupt an opponent's decision-making capability, to create doubts, foment anti-leadership sentiments, to deceive opponents and to attempt to diminish the will to fight among opponents."[53] A primary objective, as Laura Jackson explains, is "to demoralize both military personnel and civilian populations, and thus, over time, to diminish their will to act . . . to undermine international institutions, change borders, and subvert global media, all without firing a shot."[54]

China's "Three Warfares" doctrine is focused on: (1) public opinion (media) warfare (*yulun zhan*); (2) psychological warfare (*xinli zhan*); and (3) legal warfare (*falu zhan*).[55] In their conception of public opinion warfare, the goal is to influence both domestic and international public opinion in ways that build support for China's own military operations, while undermining any justification for an adversary who is taking actions counter to China's interests.[56] But this effort goes well beyond what Steven Collins refers to in a 2003 *NATO Review* article as "perception management," in which a nation or organization provides (or withholds) certain kinds of information to influence foreign public opinion, leaders, intelligence agencies, and the policies and behaviors that result from their interpretation of this information.[57] According to the Pentagon report, China "leverages all instruments that inform and influence public opinion . . . and is directed against domestic populations in target countries."[58] As Laura Jackson explains, "China's extensive global media network, most notably the Xinhua News Agency and China Central Television (CCTV), also plays a key role, broadcasting in foreign languages and providing programming to stations throughout Africa, Central Asia, Europe, and Latin America."[59] In turn, Western media outlets then repeat and amplify the spread of messages to a broader international audience, lending a perception of legitimacy to what is in fact Chinese state-directed propaganda.[60]

Similarly, Russia has also engaged in a broad, multifaceted influence warfare campaign involving all of the former tools and tactics of its active measures program along with a flurry of new technological approaches. Media outlets like Sputnik and RT (formerly Russia Today) view themselves—according to Margarita Simonyan, chief editor of RT—as equal in importance to the Defense Ministry, using "information as a weapon."[61] And like many other authoritarian regimes, Russia has invested heavily in online troll farms, armies of automated bot accounts, cyber hacking units, and other means by which they can pursue their foreign influence goals using the most modern tools available to them.[62] While the "agent of influence" of the Cold War may have been a journalist, a government official, a labor leader, or an academic (among many other examples), today the agent is more likely to be a social media user with enough followers to be considered a potential "influencer."[63]

According to a report by the Stanford Internet Observatory, both China and Russia have "full-spectrum propaganda capabilities," including prominent Facebook pages and YouTube channels targeting regionalized audiences.[64] Both have military units dedicated to influencing foreign targets and also encourage and incentivize citizen involvement in those efforts.[65] They gather extensive information about their targets and manage an array of fake Facebook pages and Twitter personas that are used for eroding the international perception and domestic social cohesion of its rivals.[66] And as detailed in many reports by congressional committees, think tanks, and academics, Russia has been particularly aggressive during this past decade in its online efforts to influence democratic elections in the United States, Europe, Africa, and elsewhere, as well as to sow confusion and encourage widespread societal polarization and animosity.[67]

Meanwhile, other countries are also increasingly engaging in their own forms of digital influence warfare. In October 2019, Facebook announced the deletion of 93 Facebook accounts, 17 Facebook pages, and 4 Instagram accounts "for violating our policy against coordinated inauthentic behavior. This activity originated in Iran and focused primarily on the US, and some on French-speaking audiences in North Africa."[68] According to the announcement, "the individuals behind this activity used compromised and fake accounts—some of which had already been disabled by our automated systems—to masquerade as locals, manage their Pages, join Groups and drive people to off-platform domains connected to our previous investigation into the Iran-linked 'Liberty Front Press' and its removal in August 2018."[69] Facebook also removed 38 Facebook accounts, 6 pages, 4 groups, and 10 Instagram accounts that originated in Iran and focused on countries in Latin America, including Venezuela, Brazil, Argentina, Bolivia, Peru, Ecuador, and Mexico. The page administrators and account owners typically represented themselves as locals, used fake accounts to post in groups and manage pages posing as news organizations, as well as directed traffic to other websites.[70] And that same month, Microsoft announced that hackers linked to the Iranian government targeted an undisclosed U.S. presidential campaign, as well as government officials, media outlets, and prominent expatriate Iranians.[71]

In short, older strategies, tactics, and tools of influence warfare have evolved to encompass a new and very powerful digital dimension. By using massive amounts of internet user data, including profiles and patterns of online behavior, microtargeting strategies have become a very effective means of influencing people from many backgrounds. The strategies, tactics, and tools of digital influence warfare will increasingly be used by foreign and domestic actors to manipulate our perceptions in ways that will negatively affect us. According to a 2018 United Nations Educational, Scientific and Cultural Organization (UNESCO) report, the danger we face in the future is "the development of an 'arms race' of national and international disinformation spread through partisan 'news' organizations and social media channels, polluting the information environment for all sides."[72]

Tomorrow's disinformation and perceptions manipulation will be much worse than what we are dealing with now, in part because the tactics and tools are becoming more innovative and sophisticated. As a 2019 report by Rand notes, "Increasingly, hostile social manipulation will be able to target the information foundations of digitized societies: the databases, algorithms, networked devices, and artificial intelligence programs that will dominate the day-to-day operation of the society."[73] The future evolution of digital influence tools—including augmented reality, virtual reality, and artificial intelligence (AI)—promise to bring further confusion and challenges to an already chaotic situation, offering a new frontier for disinformation and perceptions manipulation.[74] For example, in the not-too-distant future we will see a flood of fake audio, images, messages, and video created through AI that will appear so real it will be increasingly difficult to convince people they are fakes.[75] Technology already exists that can be used to manipulate an audio recording to delete words from a speech and then stitch the rest together seamlessly, or add new words using software that replicates the voice of the speaker with uncanny accuracy.[76] Imagine the harm that can be done when in the future, digital influencers have the ability to clone any voice, use it to say anything the influencer wants, and then use that audio recording to persuade others.[77]

Creating deepfake images and video is also becoming easier, with increasingly realistic results becoming more convincing. One particularly sophisticated AI-related approach involves a tool known as generative adversarial networks (GANs). These involve integrating a competitive function into software, with one network seeking to generate an item, such as an image or video, while the other network judges the item to determine whether it looks real. As the first network continues to adapt to fool the adversarial network, the software learns how to better create more realistic images or videos.[78] Over time, according to Michael Mazzar and his colleagues at Rand, "As technology improves the quality of this production, it will likely become more difficult to discern real events from doctored or artificial ones, particularly if combined with the advancements in audio software."[79] If the target of such deepfake disinformation holds true to the old adage of "hearing and seeing is believing," the long-term harmful effects of this technology are quite obvious. Technological advances will make it increasingly difficult to distinguish real people from computer-generated ones, and even more difficult to convince people that they are being deceived by someone they believe is real.

And, of course, we can fully expect that digital influence warfare attacks against democratic elections will continue and will likely involve new and innovative tactics. For example, there are concerns that in the future malicious hackers could use ransomware to snatch and hold hostage databases of local voter registrations or cause power disruptions at polling centers on election day. Further, as one expert noted, "with Americans so mistrustful of one another, and of the political process, the fear of hacking could be as dangerous as an actual cyberattack—especially if the election is close."[80] As Laura Rosenberger observes, "You don't actually have to breach an election system in order to create the public impression that you have."[81] The future will likely bring darker influence silos that no light of truth can penetrate, resulting in heightened uncertainty and distrust, deeper animosity, more extremism and violence, and widespread belief in things that simply are not true. This is the future that the enemies of America's peace and prosperity want to engineer. The United States must find ways to prevent them from succeeding. The research and analysis provided in this issue contributes to that important goal.

The Issue of *JAMS* on Political Warfare and Propaganda

Each of the contributions to this issue addresses the central theme of influencing perceptions and behavior. First, Daniel de Wit draws lessons from a historical analysis of the Office of Strategic Services (OSS), America's intelligence and special operations organization in World War II. In addition to its efforts to collect intelligence on the Axis powers and to arm and train resistance groups behind enemy lines, the OSS also served as America's primary psychological warfare agency, using a variety of "black propaganda" methods to sow dissension and confusion in enemy ranks.[82] As noted earlier, psychological warfare plays a significant role in the conduct of today's military operations, so de Wit's research offers important historical lessons for contemporary campaign planners.

Next, Kyleanne Hunter and Emma Jouenne examine the uniquely troubling effects of spreading misogynistic views online. Their analysis of three diverse case studies—the U.S. military, the incel movement, and ISIS—reveals how unchecked online misogyny can result in physical behavior that can threaten human and national security. Glen Segell then explores how perceptions about cybersecurity operations can have positive or negative impacts on civil-military relations, drawing on a case study of the Israeli experience. Lev Topor and Alexander Tabachnik follow with a study of how Russia uses the strategies and tactics of digital influence warfare against other countries, while continually seeking to strengthen its information dominance over Russian citizens. And Donald M. Bishop reveals how other countries do this as well, including China, North Korea, Iran, Cuba, and Venezuela. Each is engaged in these same kinds of efforts to control the information that circulates within their respective societies, while using various forms of propaganda against other countries to strengthen their influence and national power.

Phil Zeman's contribution to this issue looks at how China and Russia are trying to fracture American and Western societies through information, disinformation, economic coercion, and the creation of economic dependencies—in many cases capitalizing on specific attributes and vulnerabilities of a target nation to achieve their strategic objectives. Through these efforts, he concludes, China and Russia hope to prevent the will or ability of American or Western states to respond to an aggressive act. Next, Michael Cserkits explains how a society's perceptions about armed forces can be influenced by cinematic productions and anime, drawing on a case study comparison of Japan and the United States. And finally, Anthony Patrick examines how social media penetration and internet connectivity could impact the likelihood that parties within a conventional intrastate conflict will enter negotiations.

As a collection, these articles make a significant contribution to the scholarly research literature on political warfare and propaganda. The authors shed light on the need for research-based strategies and policies that can improve our ability to identify, defend against, and mitigate the consequences of influence efforts. However, when reflecting on the compound security threats described at the beginning of this introduction—involving both cyberattacks and influence attacks—a startling contrast is revealed: we have committed serious resources toward cybersecurity but not toward addressing the influence issues examined in this issue. We routinely install firewalls and other security measures around our computer network systems, track potential intrusion attempts, test and report network vulnerabilities, hold training seminars for new employees, and take many other measures to try and mitigate cybersecurity threats. In contrast, there are no firewalls or intrusion detection efforts defending us against digital influence attacks of either foreign or domestic origin. Government sanctions and social media deplatforming efforts respond to influence attackers once they have been identified as such, but these efforts take place after attacks have already occurred, sometimes over the course of several years.

The articles of this issue reflect an array of efforts to influence the perceptions, emotions, and behavior of human beings at both individual and societal levels. In the absence of comprehensive strategies to more effectively defend against these efforts, the United States risks losing much more than military advantage; we are placing at risk the perceived legitimacy of our systems and institutions of governance, as well as our economic security, our ability to resolve social disagreements peacefully, and much more.[83] Further, many other nations are also facing the challenges of defending against foreign influence efforts. As such, the transnational nature of influence opportunities and capabilities in the digital age may require a multinational, coordinated response. In the years ahead, further research will be needed to uncover strategies for responding to the threat of digital influence warfare with greater sophistication and success.

Endnotes

[1] Marshall McLuhan, *Culture Is Our Business* (Eugene, OR: Wipf and Stock Publishers, 1970), 66.

[2] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: Rand, 2001), 1, https://doi.org/10.7249/MR1382.

[3] Isaiah Wilson III, "What Is Compound Security?: With Dr. Isaiah 'Ike' Wilson III (Part 2 of 4)," YouTube, 26 February 2021, 16:48; and Isaiah Wilson III and Scott A. Smitson, "The Compound Security Dilemma: Threats at the Nexus of War and Peace," *Parameters* 50, no. 2 (Summer 2020): 1–17.

[4] Wilson, "What Is Compound Security?"; and Wilson and Smitson, "The Compound Security Dilemma."

[5] Max Boot and Michael Doran, "Political Warfare," Council on Foreign Relations, 28 June 2013.

[6] Paul A. Smith, *On Political War* (Washington, DC: National Defense University Press, 1989), 3.

[7] Carnes Lord, "The Psychological Dimension in National Strategy," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Carnes Lord and Frank R. Barnett (Washington, DC: National Defense University Press, 1989), 16.

[8] *Military Information Support Operations*, Joint Publication 3-13.2 (Washington, DC: Joint Chiefs of Staff, 2014).

[9] Diego A. Martin and Jacob N. Shapiro, *Trends in Online Foreign Influence Efforts* (Princeton, NJ: Woodrow Wilson School of Public and International Affairs, Princeton University, 2019), 3.

[10] Martin and Shapiro, *Trends in Online Foreign Influence Efforts.*

[11] Martin and Shapiro, *Trends in Online Foreign Influence Efforts.*

[12] Philip N. Howard, *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives* (New Haven, CT: Yale University Press, 2020), 75.

[13] Caroline Jack, *Lexicon of Lies: Terms for Problematic Information* (New York: Data & Society Research Institute, 2017), 6.

[14] Carl Miller, *The Death of the Gods: The New Global Power Grab* (London: Windmill Books, 2018), xvi.

[15] Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (Abingdon, UK: Routledge, 2019), 11.

[16] Michael V. Hayden, *The Assault on Intelligence: American National Security in an Age of Lies* (New York: Penguin Press, 2018), 191.

[17] In addition to terrorists and insurgents using these tools of digital influence for political purposes, we also see various kinds of individuals and marketing firms engaged in profit-seeking activities as described in James J. F. Forest, *Digital Influence Mercenaries: Profit and Power Through Information Warfare* (Annapolis, MD: Naval Institute Press, 2021).

18. James. J. F. Forest, ed., *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas* (Westport, CT: Praeger Security International, 2009).
19. While Arquilla and Ronfeldt initially defined *swarming* as a "deliberately structured, coordinated, strategic way to strike from all directions," in this context the term is used to describe a collection of social media accounts that converges on a single target like a swarm of bees. See John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: Rand, 2000); Ali Fisher, "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence," *Perspectives on Terrorism* 9, no. 3 (June 2015): 3–20; and *bandwagoning* is a term from social psychology used to describe a type of cognitive bias and collective identity signaling that leads people to adopt the behaviors or attitudes of others. This can be observed in political campaigns, support for a winning sports team, fashion trends, adoption of new consumer electronics, and many other arenas of daily life.
20. James J. F. Forest, *Digital Influence Warfare in the Age of Social Media* (Santa Barbara, CA: ABC-CLIO/Praeger Security International, 2021).
21. Specifically, chapter 3, "Attack by Strategem" reads: "Supreme excellence consists in breaking the enemy's resistance without fighting." Sun Tzu, *The Art of War* (New York: Fall River Press, 2015), 54.
22. Galeotti, *Russian Political War*, 10.
23. Russell Hsiao, "CCP Propaganda against Taiwan Enters the Social Age," *China Brief* 18, no. 7 (April 2018).
24. W. Phillips Davison, "Some Trends in International Propaganda," *Annals of the American Academy of Political Science and Social Science* 398, no. 1 (November 1971): 1–13, https://doi.org/10.1177/000271627139800102.
25. Daniel Baracskay, "U.S. Strategic Communication Efforts during the Cold War," in *Influence Warfare*, 253–74.
26. James Woods, *History of International Broadcasting*, vol. 2 (London: IET, 1992), 110.
27. Woods, *History of International Broadcasting*, 110–11.
28. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Strauss and Giroux, 2020), 4.
29. Rid, *Active Measures*, 7.
30. Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (New York: Pergamon Brassey's, 1984), 133.
31. Shultz and Godson, *Dezinformatsia*, 133.
32. Shultz and Godson, *Dezinformatsia*, 149.
33. Shultz and Godson, *Dezinformatsia*, 150–51.
34. Shultz and Godson, *Dezinformatsia*, 152–53.
35. Shultz and Godson, *Dezinformatsia*, 155.
36. Shultz and Godson, *Dezinformatsia*, 157.
37. This is a cornerstone of Russia's digital influence warfare program and the title of an important book. See Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia* (New York: Public Affairs, 2014).
38. This section of the discussion significantly amplifies and paraphrases a report by Eric V. Larson et al., *Understanding Commanders' Information Needs for Influence Operations* (Santa Monica, CA: Rand, 2009), Appendix B: Task List Analysis, 71–73, which cites several Department of the Army documents and 1st Information Operations Command (Land), Field Support Division, "Terminology for IO Effects," in *Tactics, Techniques and Procedures for Operational and Tactical Information Operations Planning* (Washington, DC: Department of the Army, 2004), 23.
39. Larson et al., *Understanding Commanders' Information Needs for Influence Operations*, 71–73.
40. For details, see Forest, *Digital Influence Mercenaries.*
41. Howard, *Lie Machines*, 99–100. *Junk news* was defined by the Oxford Internet Institute as being articles from outlets that publish "deliberately misleading, deceptive or incorrect information." See Ryan Browne, " 'Junk News' Gets Massive Engagement on Facebook Ahead of EU Elections, Study Finds," CNBC, 21 May 2019.

42. Elisa Shearer and Jeffrey Gottfried, "News Use Across Social Media Platforms 2017," Pew Research Center, 7 September 2017.
43. Ben Nimmo, Graham Brookie, and Kanishk Karanm, "#TrollTracker: Twitter Troll Farm Archives, Part One—Seven Key Take Aways from a Comprehensive Archive of Known Russian and Iranian Troll Operations," Atlantic Council's Digital Forensic Research Lab, 17 October 2018.
44. For the purpose of this discussion, a "like-minded fellow traveler" is described as someone who sees the world in much the same way you do and is moving intellectually and emotionally in a direction that you approve of.
45. Claire Wardle, "Fake News. It's Complicated," First Draft, 16 February 2017.
46. Rid, *Active Measures*, 5, with a direct quote from famous Soviet defector Ladislav Bittman, author of the 1972 book *The Deception Game* (Syracuse, NY: Syracuse University Research Corp, 1972).
47. Various interpretations of this classic work use different phrasing. For example, "If your opponent is of choleric temper, seek to irritate him." Sun Tzu, *The Art of War*, 49 (passage 1.22); and "When their military leadership is obstreperous, you should irritate them to make them angry—then they will become impetuous and ignore their original strategy." Sun Tzu, *The Art of War*, trans. by Thomas Cleary (Boston, MA: Shambhala Pocket Classics, 1991), 15 (passage 1.12).
48. For a detailed examination of this event, see David E. Sanger, *The Perfect Weapon: Sabotage and Fear in the Cyber Age* (New York: Crown Publishing, 2018), 124–43.
49. Sanger, *The Perfect Weapon*, 143.
50. Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vol. 1 (Washington, DC: Department of Justice, 2019).
51. Renee DiResta et al., *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives* (Stanford, CA: Stanford Internet Observatory and Hoover Institution, Stanford University, 2020), 3.
52. Howard, *Lie Machines*, 77; Jonathan Kaiman, "Free Tibet Exposes Fake Twitter Accounts by China Propagandists," *Guardian*, 22 July 2014; and Nicholas J. Monaco, "Taiwan: Digital Democracy Meets Automated Autocracy," in *Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media*, ed. Samuel C. Woolley and Philip N. Howard (New York: Oxford University Press, 2018), 104–27, https://doi.org/10.1093/oso/9780190931407.003.0006.
53. Stefan Halper, *China: The Three Warfares* (Washington, DC: Office of the Secretary of Defense, 2013), 12.
54. Halper, *China.*
55. Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle Barracks, PA: United States Army War College Press, 2014), 29–30. Note: according to Wortzel, a direct translation of *yulun* is "public opinion"; thus, in many English translations, the term "public opinion warfare" is used. In some People's Liberation Army translations of book titles and articles, however, it is called "media warfare."
56. Wortzel, *The Chinese People's Liberation Army and Information Warfare.*
57. Steven Collins, "Mind Games," *NATO Review* (Summer 2003).
58. Halper, *China,* 12–13.
59. Laura Jackson, "Revisions of Reality: The Three Warfares—China's New Way of War," in *Information at War: From China's Three Warfares to NATO's Narratives* (London: Legatum Institute, 2015), 5–6.
60. Jackson, "Revisions of Reality."
61. Ben Nimmo, "Question That: RT's Military Mission," Atlantic Council's Digital Forensic Research Lab, 8 January 2018.
62. *Statement Prepared for the U.S. Senate Select Committee on Intelligence Hearing, 115th* Cong. (30 March 2017) (statement of Clint Watts on "Disinformation: A Primer in Russian Active Measures and Influence Campaigns"), hereafter Watts statement.
63. Watts statement.
64. Watts statement.
65. For details on the efforts of both China and Russia, see Ross Babbage, *Winning With-*

out Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail, vol. 1 (Washington, DC: Center for Strategic and Budgetary Assessments, 2019); Esther Chan and Rachel Blundy, " 'Bulletproof' China-backed Site Attacks HK Democracy Activists," Yahoo News, 1 November 2019; John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives 13 (Washington, DC: National Defense University Press, 2018); Joanne Patti Munisteri, "Controlling Cognitive Domains," *Small Wars Journal*, 24 August 2019; Austin Doehler, "How China Challenges the EU in the Western Balkans," *Diplomat*, 25 September 2019; Keoni Everington, "China's 'Troll Factory' Targeting Taiwan with Disinformation Prior to Election," *Taiwan News*, 5 November 2018; "Hong Kong Protests: YouTube Shuts Accounts over Disinformation," BBC News, 22 August 2019; Paul Mozur and Alexandra Stevenson, "Chinese Cyberattack Hits Telegram, App Used by Hong Kong Protesters," *New York Times*, 13 June 2019; and Tom Uren, Elise Thomas, and Jacob Wallis, *Tweeting through the Great Firewall: Preliminary Analysis of PRC-linked Information Operations on the Hong Kong Protests* (Canberra: Australian Strategic Policy Institute, 2019).

66. DiResta et al., *Telling China's Story.*

67. *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution* (Washington, DC: Office of the Director of National Intelligence, 2017); Ellen Nakashima, "Senate Committee Unanimously Endorses Spy Agencies' Finding that Russia Interfered in 2016 Presidential Race in Bid to Help Trump," *Washington Post*, 21 April 2020; Jane Mayer, "How Russia Helped Swing the Election for Trump," *New Yorker*, 24 September 2018; Philip N. Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012–2018* (Oxford, UK: Programme on Democracy & Technology, 2018); and Nike Aleksejeva et al., *Operation Secondary Infektion: A Suspected Russian Intelligence Operation Targeting Europe and the United States* (Washington, DC: Atlantic Council Digital Forensic Research Lab, 2019).

68. Nathaniel Gleicher, "Removing More Coordinated Inauthentic Behavior from Iran and Russia," Facebook Newsroom, 21 October 2019.

69. Gleicher, "Removing More Coordinated Inauthentic Behavior from Iran and Russia."

70. Gleicher, "Removing More Coordinated Inauthentic Behavior from Iran and Russia."

71. "Hacking Group Linked to Iran Targeted a U.S. Presidential Campaign, Microsoft Says," *Los Angeles (CA) Times*, 4 October 2019.

72. Cherilyn Ireton and Julie Posetti, *Journalism, "Fake News" and Disinformation* (Paris: UNESCO, 2018), 18.

73. Michael J. Mazarr et al., *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment* (Santa Monica, CA: Rand, 2019), 65–66, https://doi.org/10.7249/RR2714.

74. For instance, see Rob Price, "AI and CGI Will Transform Information Warfare, Boost Hoaxes, and Escalate Revenge Porn," Business Insider, 12 August 2017; and Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 87.

75. Will Knight, "Fake America Great Again: Inside the Race to Catch the Worryingly Real Fakes that Can Be Made Using Artificial Intelligence," *MIT Technology Review* 17 August 2018; for some examples of realistic Instagram memes created by powerful computer graphics equipment combined with AI, see "the_fakening," Instagram, accessed 6 April 2021.

76. Avi Selk, "This Audio Clip of a Robot as Trump May Prelude a Future of Fake Human Voices," *Washington Post*, 3 May 2017; Bahar Gholipour, "New AI Tech Can Mimic Any Voice," *Scientific American*, 2 May 2017; and Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 85–86.

77. "Imitating People's Speech Patterns Precisely Could Bring Trouble," *Economist*, 20 April 2017; and Mazarr et al, *The Emerging Risk of Virtual Societal Warfare*, 86.

78. "Fake News: You Ain't Seen Nothing Yet," *Economist*, 1 July 2017; Faizan Shaikh, "Introductory Guide to Generative Adversarial Networks (GANs) and Their Promise!,"

Analytics Vidhya, 15 June 2017; and Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 88.

79. Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 91.

80. Matthew Rosenberg, Nicole Perlroth, and David E. Sanger, " 'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020," *New York Times*, 10 January 2020.

81. Rosenberg, Perlroth, and Sanger, " 'Chaos Is the Point'."

82. Howard Becker, "The Nature and Consequences of Black Propaganda," *American Sociological Review* 14, no. 2 (April 1949): 221, https://doi.org/10.2307/2086855. " 'Black' propaganda is that variety which is presented by the propagandizer as coming from a source inside the propagandized."

83. For a discussion of strategies to counter foreign influence threats from Chinese and Russian malign influence efforts, see Thomas G. Mahnken, Ross Babbage, and Toshi Yoshihara, *Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare* (Washington, DC: Center for Strategic and Budgetary Assessments, 2018).

Fake News for the Resistance
The OSS and the Nexus of Psychological Warfare and Resistance Operations in World War II

Daniel de Wit

Abstract: The Office of Strategic Services (OSS), America's intelligence and special operations organization in World War II, is best known for its efforts to collect intelligence on the Axis powers and to arm and train resistance groups behind enemy lines. However, the OSS also served as America's primary psychological warfare agency. This article will show how organizational relationships imposed by theater commanders, who often had little understanding of psychological warfare or special operations, could serve to enable or hinder the sort of coordinated subversive campaign that OSS founder General William J. Donovan envisioned. This history offers important lessons for contemporary campaign planners in an environment where psychological warfare is playing an ever-larger role in the conduct of military operations.

Keywords: psychological warfare, unconventional warfare, information operations, influence, the human domain

The Office of Strategic Services (OSS), America's World War II-era intelligence and special operations organization, enjoys justifiable acclaim for its exploits behind enemy lines. Initiatives such as Operation Jedburgh, the multinational operation to leverage French resistance units to disrupt the German response to the D-Day landings, continue to be explored in both popular histories and military studies seeking to develop lessons for the current

Daniel de Wit is an operations support officer at the Defense Intelligence Agency, an officer in the Marine Corps Reserve, and a PhD candidate in War Studies at King's College London. The views presented here are his alone and do not reflect the position of the Defense Intelligence Agency or the U.S. Marine Corps.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201002

operating environment.[1] In contrast, the OSS's psychological warfare section, the Morale Operations Branch, has received far less attention from both popular and scholarly historians.[2] This is unfortunate, as Major General William J. Donovan, the Wall Street lawyer and war hero of World War I who founded the OSS and led it through the course of the war, saw psychological warfare and support to resistance groups (now known as "unconventional warfare" in American doctrine) as two sides of the same coin. These were meant to be employed in a cohesive manner to undermine enemy forces prior to the start of conventional military operations—or what practitioners at the time referred to as "subversive warfare."[3] And yet, despite the fact that Donovan designed the OSS to be able to conduct these functions together, with both the Special Operations (SO) and Morale Operations (MO) Branches falling under a deputy director for psychological warfare, the OSS's record of conducting combined operations by these two branches was wildly uneven.[4] In some theaters, particularly in Burma and China, the MO and SO Branches were able to operate in integrated teams that leveraged the skills of both. In the European theater, in contrast, the Morale Operations Branch played almost no role in support of resistance operations and was relegated to a minor role alongside other propaganda and public affairs elements on the staff of the Supreme Headquarters Allied Expeditionary Force (SHAEF). As the following sections will show, this variance was due entirely to the command relationships between OSS regional offices and the military theater commanders in those regions, and the resulting organizational constructs that either encouraged and facilitated cohesion between OSS branches or divorced them from each other and forced the Morale Operations Branch to the sidelines under leaders who did not know how to employ it. Indeed, the MO and SO Branches enjoyed a close working relationship in the Mediterranean and China-Burma-India (CBI) theaters, while they were severed in the European theater. In Burma and the Mediterranean, British commanders well-versed in irregular warfare gave OSS a relatively free hand to fight the war on its terms, while American general Joseph W. Stilwell, the U.S. commander in Burma, was fighting an economy-of-force effort and relied on OSS so heavily that he had little ability to interfere in its methods.

The OSS case is instructive for the current era of competition between adversarial great powers as it shows how commanders who lack an understanding of psychological and unconventional warfare and are determined to force them to fit a command structure designed for traditional combat arms can improperly use such an organization. Numerous studies have already shown that Russia and China seek to use military operations to achieve psychological objectives, inverting the traditional American perspective, which sees psychological warfare as an enabler to combined arms maneuver.[5] The increasing cost and lethality of conventional warfare is driving up the utility of psychological operations and other special operations functions, which can achieve strategic aims without crossing thresholds that might trigger a major war.[6] Despite this realization, much of the discussion within the Department of Defense (DOD) about how to respond to the threat posed by both of these adversaries focuses on the weapons systems and operating concepts required to win a conventional war, rather than on countering hostile actions and advancing our own objectives without resorting to combat operations.[7] Of course, conventional military capabilities remain a critical necessity, without which there would be nothing to deter adversaries from simply pursuing their objectives through direct military action rather than through measures short of war. However, in this threat environment populated by psychological operations used by our adversaries, conventional military commanders must have a thorough appreciation of how psychological warfare tools can supplement both special and conventional military operations. The experience of OSS's Morale Operations Branch will be eminently useful in this regard.

Organizing for Subversive Warfare

General Donovan's concept of subversive warfare originated in the years immediately prior to World War II, when Donovan was a respected Wall Street lawyer with numerous international clients and an important player in the Republican Party. Beginning in the mid-1930s, Donovan began traveling the world, ostensibly to meet with clients but really to develop his own observations of the looming breakdown in the world order and march to war—observations that he relayed directly to President Franklin D. Roosevelt on his return.[8] It was these activities that eventually resulted in his being assigned to liaise with the British intelligence services and then create a similar organization for the United States. Donovan was particularly disturbed by what he saw as the ability of fascist propaganda to undermine national cohesion and will to fight. He published his findings in a 1941 pamphlet entitled *Fifth Column Lessons for America*.[9] He argued that Nazi propaganda had played an integral role in the fall of France by convincing leftist labor elements to undermine arms production in the years prior to the war, while simultaneously undermining the officer class's will to fight and damaging morale cohesion to the point that they routinely deserted their troops rather than resist the German onslaught when it finally came in 1940.

Some historians have contested his conclusions about the efficacy of German propaganda, but it is clear that Donovan saw psychological warfare as a key precursor to successful military operations.[10] He was of the opinion that the United States could only succeed in the coming war if it had its own agency to conduct psychological and unconventional warfare as both the Germans and the British had. President Roosevelt finally agreed and directed Donovan to establish a service to house these capabilities in June 1941. The Office of the Coordinator of Information (COI), as it was initially known, was intended to consolidate the full panoply of intelligence and subversive warfare tools in a single agency. It included departments for human intelligence collection and analysis, a special operations element to conduct sabotage and guerrilla warfare, and the Foreign Information Service (FIS), which Donovan intended to be the comprehensive propaganda and psychological warfare arm of the U.S. government.[11]

The ink on the COI charter was barely dry before a major dispute arose within its ranks over the role of propaganda in a democratic government. Many of the journalists and advertising agents that Donovan hired to staff the FIS, including its director Robert Sherwood, shared President Franklin Roosevelt's center-left political philosophies, which placed great weight on the role of the United States as a beacon for enlightened democracy (in contrast to Europe, where monarchy and aristocracy enjoyed considerable power until the outbreak of the war) and saw the use of deceptive and manipulative propaganda as the morally repugnant tool of fascist regimes. They were of the opinion that the only acceptable form of propaganda in a democracy was truthful information that sought to convince audiences of the righteousness of the American example—so called white propaganda.[12] They were also opposed to close coordination with the Armed Services—a position obviously at odds with Donovan's own.[13] This dispute was so intractable that within months, FIS effectively became a department in revolt against its parent agency and the issue required direct intervention from President Roosevelt. A year after the COI was founded, Roosevelt issued an executive order splitting it into two new organizations: the FIS became the independent Office of War Information (OWI), which dealt exclusively in white propaganda. The remaining elements became the OSS, which was then directed by the Joint Chiefs of Staff in December 1942 to establish its own black propaganda arm to support military operations.[14] The Morale Operations Branch was officially created in early 1943, though problems of recruitment, training, and supply meant that its officers would not start making an impact in the field until mid-1944.

Donovan's vision for the Morale Operations Branch was that it should operate in close coordination with the Special Operations Branch. Together, these branches would conduct a phased campaign of subversive operations to undermine Axis forces prior to major offensives by Allied forces. Donovan summed up this concept as follows:

> propaganda is the arrow of initial penetration in conditioning and preparing the people and territory in which invasion is contemplated. It is the first step—then Fifth Column work [meaning sabotage and guerrilla warfare behind enemy lines],

> then militarized raiders (or 'Commandos'), and then the invading divisions.[15]

This concept was codified in the Morale Office Branch manual, which directed its officers to operate "in close liaison" with the Special Operations Branch and to use Special Operations Branch agents and underground networks to "assist in the promotion of resistance and revolt among people of enemy-occupied and controlled territory."[16]

However, as the following sections will show, their ability collaborate effectively varied from theater to theater depending on the organizational restrictions imposed by the theater commanders. This is despite the fact that both guerrilla and psychological warfare organizations were housed within the same agency and the branches assigned these roles received clear guidance to collaborate in their subversive campaigns.

Conventional Perspectives on Special Operations

Due to a combination of factors arising out of the military culture and the professional military education of American military officers during the interwar period, the American general officers who oversaw the U.S. contribution to the war effort at the corps level and above had no concept of, let alone training in, special operations and psychological warfare. This left them poorly positioned to oversee OSS operations in their respective theaters. The U.S. Army's official history of special operations in World War II makes clear how unfamiliar the Army was with special operations and notes that the officer corps of the period was preoccupied with questions of mass mobilization and the maneuver of large conventional formations on the battlefield.[17] The universally agreed-on theory of victory was for the Army to mass sufficient combat power to destroy the enemy's forces in the field. The history goes on to note:

> Unconventional operations, with their elements of stealth, secrecy, and political complications, seemed foreign, even devious, to officers accustomed to straightforward conventional tactics and the interwar Army's ordered, gentlemanly world of polo and bridge.[18]

The culture of the American officer corps during the period was conservative to the point of being hidebound, likely a protective instinct in response to post–World War I force reductions and budget cuts.[19] This attitude prevailed well into World War II. Historian Alfred H. Paddock quotes an unsigned letter in the records of the Western Task Force in 1942 in which an officer stated their firm opinion that

> The only propaganda which can achieve results is the propa-

> ganda of deeds not words. One medium tank has proved far more effective than all the bag of trick gadgets [*sic*], which merely offend good taste and give nothing concrete where want is great.[20]

This mindset was reinforced by the professional military education of the period, which was focused on ways to mass sufficient combat power at the decisive point on the battlefield while maintaining operational mobility and avoiding the trench warfare of the western front. For example, a lecture on the principles of war given annually from 1923 to 1927 at the Army's Command and General Staff School at Fort Leavenworth and was attended by General Dwight D. Eisenhower, all 6 of his army commanders, and 25 of 34 corps commanders noted that "the first consideration under the principle of the objective is to determine the centers of gravity of the enemy's power. Then against this center of gravity the concentrated blow of all the forces must be directed."[21] This lecture went on to note that "the will of the people to carry on a war may be the real center of gravity of a nation, but in this situation the quickest way to reach that will is by a defeat of the hostile main forces."[22]

Given that they came up through the ranks with this background of training and military culture, it is little wonder that American general officers lacked the vocabulary necessary to even think about special operations and psychological warfare in a proactive manner. Indeed, in early 1942, General Joseph Stilwell, commander of American and Chinese forces in Burma (and, ironically, the commander of the theater in which some of the most successful combined psychological and unconventional warfare operations were to take place), stated that he had no interest in employing an OSS special operations team in support of his conventional operations.[23] He also professed to a fellow officer to have no idea what psychological warfare was, no desire to learn, and no intention of even allowing a psychological warfare element to enter his theater of operations.[24] In a similar vein, General Douglas MacArthur, commanding troops in the Southwest Pacific Theater, was unwilling to allow the presence of any intelligence or special operations unit that he did not control directly through the conventional planning framework in his general staff.[25] As a result, he barred OSS from having a presence of any kind in the Southwest Pacific Theater for the entirety of the war.

This conservative mentality stands in stark contrast to that evinced by British commanders during the same period. Britain had a lengthy history with irregular warfare techniques. While British commanders had been exceedingly suspicious of such techniques in decades past, by 1940 they showed a willingness to employ these methods to their full effect in order to hinder Nazi Germany's advance and then to undermine its cohesion. The most famous British exponent of irregular warfare was Major T. E. Lawrence, who helped lead the Arab Revolt against Ottoman rule in 1916–18. In addition to Lawrence, British officers such as Lieutenant Colonel Gerard E. Leachman and Captain William Henry Shakespear conducted operations against Ottoman rule by leveraging local militias from across Mesopotamia and the Arabian Peninsula.[26] These officers built on a foundation of nearly two centuries of colonial rule from India to South Africa that was exercised through local levies and armies of native troops. Their experiences would eventually feed directly into British special operations doctrine when, in early 1939, Lieutenant Colonel Colin M. Gubbins, a British officer with experience in irregular conflicts in Ireland and against the Bolsheviks in Russia, conducted an extensive study of these operations, which he used to draft a series of manuals for the conduct of irregular warfare and special operations.[27]

With the outbreak of World War II and the British Army's evacuation from Europe at Dunkirk in May 1940, British leaders saw a need for a special unit that could continue to prosecute the war in Europe via sabotage and guerrilla warfare. The British Ministry of Economic Warfare took on this task and established the Special Operations Executive (SOE) in July 1940 with a mandate to conduct sabotage and guerrilla warfare across occupied Europe.[28] Gubbins was swiftly brought on board and placed in charge of training the organization's new recruits before eventually taking command of SOE.[29] The SOE never had a mandate to conduct psychological warfare, but it established a close working relationship with an agency that did: the Political Warfare Executive (PWE), which was established approximately a year after SOE to oversee the full array of British propaganda operations.[30] To enable the dissemination of black propaganda materials (including leaflets and other documents designed to appear as though they originated in German or Italian presses), SOE and PWE agreed to jointly select and train a cadre of officers in techniques both of guerrilla warfare and black propaganda dissemination so that they could integrate with SOE teams being inserted by parachute into Axis-occupied territory.[31]

This divergence between British and American approaches to special operations is the primary factor that accounts for the varied experiences of OSS Morale Operations teams during the course of the war. As the following sections will show, the Morale Operations Branch was able to integrate closely with its Special Operations Branch colleagues in those theaters under British command (including the Mediterranean theater and Southeast Asia Command). In contrast, the Morale Operations Branch played a very limited role in the European theater under General Eisenhower, as the branch was forced into a conventional command structure alongside white propaganda organizations that did not know how to use its capabilities, preventing effective coordination with the Special Operations Branch. Finally, the experience of both branches in the China-Burma-India theater is the exception that proves the rule: as noted above, General Stilwell was loath to employ unconventional and psychological warfare. Both branches were forced on him by leaders in Washington, however, and he had so little in the way of functioning conventional formations at his disposal that he had no choice but to rely on their services to wage an effective campaign against the Japanese occupation of Burma.

The European Theater of Operations

The Morale Operations Branch's experience in the European theater was, by all accounts, an exercise in frustration. The command relationships that were to hamper operations in this theater were first imposed during the American campaign in Morocco and Tunisia in 1942–43. As with other American leaders, General Eisenhower, in command of the American expeditionary force in North Africa, had no training in psychological warfare and only a basic understanding of its function. Unlike many of his fellow officers, however, he was determined to keep an open mind and allowed the Office of War Information to conduct white propaganda operations alongside the Army's own tactical psychological warfare teams. The Army broadcast white propaganda messages in the immediate vicinity of regular maneuver units already under Eisenhower's command. The OSS's Morale Operations Branch was still in its infancy during this period and played barely any role in the North African campaign. To manage these functions efficiently, Eisenhower consolidated them with his public affairs officers into a Psychological Warfare Branch (PWB) on his staff, under Brigadier General Robert A. McClure.[32] The consolidation of white propaganda functions with public affairs was logical: both functions deal in the production and dissemination of messages that can be clearly attributed to the agency creating it. This organizational construct would, however, significantly hamper Morale Operations Branch's black propaganda operations once Eisenhower moved his headquarters to London in early 1944 to take command of the Supreme Headquarters Allied Expeditionary Force and prepare for the invasion of occupied Europe.

Once SHAEF was activated, the Psychological Warfare Branch was expanded into a Psychological Warfare Division (PWD), which included OWI and the Army's psychological warfare teams as well as their British counterparts from the Political Warfare Executive.[33] The PWD retained the white propaganda focus that it had employed as PWB in North Africa. The PWD official history, prepared by its officers at the end of the war, goes so far as to say that its mission was only to

> utilize all . . . available media for the simple purpose of telling the various audiences what the Supreme Commander wished

> them to do, why they should do it, and what they could expect if they carried out the Supreme Commander's wishes.[34]

Such a mission statement is indistinguishable from the standard role of a public affairs officer and leaves no room for the use of black propaganda to undermine enemy cohesion and morale. This same history goes on to state that "truth is the most important ingredient in psychological warfare."[35]

This attitude encouraged a direct, attrition-based approach to the conduct of psychological warfare at the tactical level. Rather than attempting to sow confusion within enemy ranks about the plans and intentions of their own superiors, as Morale Operations doctrine emphasized, PWD focused on using simple, direct messaging to encourage enemy troops to surrender by convincing them of the hopelessness of their situation. Its tools were viewed as simply another weapon system designed to attrite enemy forces, the only difference being that it did so in a nonlethal manner. This is evident from the emphasis in PWD training manuals on the use of leaflets, delivered by bomber or modified artillery shell, carrying the simple message that Germany's cause was lost and that the leaflet would serve as a "safe conduct pass" across Allied lines for those seeking to surrender.[36] In effect, leaflets were viewed as a nonlethal form of indirect fire, to be employed to accomplish the same goal as conventional artillery (demoralizing the adversary) but without the attendant destruction. This approach meshed well with normal Army planning processes but was altogether different from the way that Morale Operations Branch conceived of the role of black propaganda.

By the time of PWD's activation in early 1944, the Morale Operations Branch had developed a trained cadre of black propaganda specialists and established a section within OSS's London office. To ensure that this section was able to integrate into the SHAEF command structure, OSS/London was reluctantly forced to place its Morale Operations section under PWD's chain of command, separating it from the rest of its operational sections, which fell under a separate Special Forces Headquarters (SFHQ).[37] This move placed Morale Operations/London under the command of white propaganda specialists who did not know how to employ black propaganda and significantly hampered coordination with OSS's Special Operations Branch in London, which was then preparing to send officers into occupied France as part of Operation Jedburgh. Morale Operations/London was not able to begin planning to deploy officers to France to disseminate black propaganda materials on the ground until mid-July 1944, more than a month after the Operation Jedburgh teams parachuted into France to link up with French resistance groups.[38] The Morale Operations team did not actually arrive in France until just before the liberation of Paris on 25 August 1944.[39] The result was that the Morale Operations Branch was, in the words of one historian, "irrelevant to the Normandy landings."[40] Rae H. Smith, chief of Morale Operations/London, went so far as to say that his team "lost its identity" when it was placed under PWD control.[41] Unable to conduct effective psychological warfare with the Special Operations Branch behind German lines, Morale Operations/London focused the majority of its effort on finding ways to deploy black propaganda directly into Germany via radio and by dropping materials from bombers. These included a radio broadcast purporting to come from General Ludwig Beck, a highly respected German officer who was executed for his role in the July 1944 attempt to assassinate Adolf Hitler but who, according to the Morale Operations broadcast, was in fact in hiding and leading the German resistance to the Nazi regime. The Morale Operations Branch also produced German-language newspapers that were printed to appear German in origin and contained large amounts of subversive material mixed in with factual information to counter the rosy picture of the war that Nazi propagandists provided to their own troops. These were dropped across Germany during bombing missions.[42] These sorts of operations are less reliable than black propaganda deployed on the ground since material heard on the radio or found in a newspaper is not as easily internalized by the target audience as that which comes from a trusted human source and relayed face-to-face. The OSS officers also had to rely on the reports of prisoner interrogations to try to assess the impact of these operations.[43] This contrasted with the experience of Morale Operations officers deployed behind enemy lines as they could observe the impact of their actions much more immediately and make any necessary corrections to their methods in the field. It is for this reason that Morale Operations sections in other theaters sought to deploy teams as far forward as possible, where they could use locally recruited agents to disseminate black propaganda materials.

Only two small Morale Operations elements played any sort of active role on the ground in the European theater, although they did not do so behind the lines with the Special Operations Branch but rather operating from friendly or neutral territory. The first of these was a two-man team composed of OSS officers of Swedish descent who were sent under diplomatic cover to work out of the U.S. embassy in neutral Sweden.[44] These officers were able disseminate an array of rumors and subversive material to German garrisons in Norway, Denmark, and Germany using both British SOE teams (which by an early agreement with OSS had primacy in this area) and networks of their own locally developed contacts. The second was a team of several dozen officers and enlisted personnel attached to the headquarters of the 12th Army Group in August and September 1944 during the liberation of Paris and the march toward the German border.[45] The principal mission of this force was to recruit local agents on a short-term basis and use them to disseminate deceptive rumors about the direction of the 12th Army Group's advance. This team was attached to the 12th

Army Group headquarters because only OSS had a mandate to conduct black propaganda operations, while the Army's tactical psychological warfare teams (which routinely operated in direct support of conventional formations like the 12th Army Group) lacked the mandate to do so.[46] This team also used its locally recruited agents to disseminate a forged German order directing officers to abandon their troops and save themselves to preserve a core officer class in postwar Germany (a course of action that General Erich Ludendorff had actually advocated in the waning stages of World War I). Such forged orders could reasonably be expected to sow dissension and distrust among German enlisted ranks, but these and other leaflets disseminated by Morale Operations/London "were never heard from again," so it is impossible to assess their impact.[47]

The Mediterranean Theater

OSS Morale Operations flourished in the Mediterranean theater, which included operations in southern France, Italy, and the Balkans. This was in no small part due to the fact that the theater commanders did not replicate the command structures that severed the Morale Operations Branch from the rest of the OSS elements operating in theater. Once Eisenhower assumed command of SHAEF in January 1944, the Mediterranean theater passed to British field marshal Henry Maitland Wilson. Wilson had no direct experience with special operations, but he had spent the previous year as commander in chief, Middle East theater in Cairo, where he oversaw combat operations in Egypt, the Levant, and the Greek Islands. This would have included command of multiple British special operations units, such as the Special Air Service, Special Boat Squadron, and Long Range Desert Group.[48] As a result, he would have been more familiar than Eisenhower with the role that special operations units could play in support of conventional campaigns, and he did not seek to force them into command relationships that hindered their operations. Instead, under Wilson's command, Allied Forces Headquarters in Algiers (AFHQ), the Mediterranean counterpart to SHAEF, established the Special Projects Operations Center, which brought all subversive warfare elements of both the British and American militaries into a single planning section on the theater command's staff.[49] This removed the physical and institutional barriers to coordination that existed in the European theater, allowing the Morale Operations section in this theater to conduct numerous operations in close coordination with both OSS/Special Operations and British SOE teams.

OSS psychological warfare efforts in this theater began in earnest in June 1944, after Italian dictator Benito Mussolini was forced to resign and Italy formally defected to the Allies. The SPOC relocated from Algiers to Rome, from where it was able to oversee operations into German-occupied northern Italy, Yugoslavia, and Crete. As in the European theater, the objective in these operations was to convince the German rank and file that they were being abandoned by both their officers and the society that they were defending. For example, in early 1944, SOE contrived with resistance forces on occupied Crete to capture General Heinrich Kreipe, the commander of the German airborne division occupying the island.

A Morale Operations team worked with the SOE officers conducting the kidnapping to spread rumors across the island, suggesting that Kreipe had willingly defected to the British. A six-person Morale Operations team later deployed to Crete alongside SOE to assess the effectiveness of this campaign; they found that only 20 percent of the 15,000-troop occupation force could be relied on to defend the island from an Allied assault.[50] When German general Franz Krech was killed by resistance forces in mainland Greece, Morale Operations/Rome played a variation on this theme by distributing forged German newspapers claiming that Krech was executed by the Gestapo before he could defect to the Allies. The Morale Operations also distributed throughout Greece and Yugoslavia a forged letter in which Krech supposedly claimed that the German cause was lost and that continued sacrifices would be in vain.[51]

The Morale Operations Branch was handed a golden opportunity to capitalize on these themes when Allied intelligence received word of the failed attempt by German Army officers to assassinate Hitler on 20 July 1944. The Morale Operations officers recognized that if they moved quickly—while the loyalties of the German officer corps were still uncertain—it could sow widespread confusion and distrust among German units far removed from the locus of the actual conspiracy in Berlin. The Morale Operations officer Barbara Lauwers, a Czech refugee and journalist recruited into the OSS shortly after Pearl Harbor for her language and writing abilities, initiated Operation Sauerkraut within a matter of hours of the failed assassination attempt. The operation sought to sow confusion and dissension in German ranks by claiming, through an array of forged orders and seemingly official announcements, that Field Marshal Walther von Brauchitsch was taking command of the German Army and instigating a full-scale revolt against the *Schutzstaffel* (SS) and other elements of the Nazi regime.[52] To make this narrative as convincing as possible, Lauwers recruited 16 German prisoners of war (POWs) from nearby POW camps, issued them cover stories and corresponding uniforms and equipment, and arranged for Special Operations Branch officers to escort them north to German lines where they were able to reinfiltrate German forces and distribute thousands of pages of forged documents.[53] One of these agents was able to return to Allied lines. After distributing his propaganda material, he reported that the message was being read and generating confusion and heated debate even among the Nazi regime's most loyal troops in the SS.

As part of Operation Sauerkraut, Lauwers also designed a messaging campaign aimed at convincing German troops that their wives and girlfriends back home were routinely being promiscuous and unfaithful. This message was deployed through a series of leaflets and letters advertising an "Association of Lonely War Women" who would be willing to do their patriotic duty by engaging in short-term dalliances with German troops on leave from the front.[54] The advertisement closed by saying,

> We, of course, are selfish too—we have been separated from our men for many years. With all those foreigners around us, we would like once more to press a real German youth to our bosom. No inhibitions now: Your wife, sister, or lover is one of us as well.[55]

A statement like this was, of course, all but guaranteed to undermine the trust of the German soldier reading it in the fidelity of loved ones back home and perhaps cause him to question what he was fighting for or what he had to come home to when the war was done.

The effect of these operations on the already strained morale of German forces in Italy can be seen in the results of one of the few air-dropped leaflet operations of the Italian campaign. Morale Operations/Rome designed a leaflet purporting to be issued by the Yugoslav Partisans under the command of Josip Broz Tito, a resistance group operating in northern Italy near the lines of the fascist *Monterosa Division*, which had remained loyal to Mussolini and to Germany after Italy formally capitulated in 1944. These leaflets granted the bearer safe conduct through partisan lines to surrender. More than a thousand soldiers from the *Monterosa Division* surrendered within a week of the leaflets being dropped.[56] Further desertions were limited only by the Yugoslav Partisans ability to house and feed surrendering troops. Lauwers was eventually awarded a Bronze Star for her efforts.

The China-Burma-India Theater

The CBI theater would prove to be the venue for the most closely integrated operations between the Morale Operations and Special Operations Branches. As in the Mediterranean theater, this was due largely to the prevailing command relationships, which—both by accident and by design—gave OSS maximum flexibility to pursue its operations in accordance with Donovan's vision for integrated operations. The CBI theater suffered from some of the most convoluted command relationships of the war, especially where intelligence and special operations functions were concerned. Burma and India were still considered British colonies and therefore fell under the British-led Southeast Asia Command (SEAC) of Admiral Lord Louis Mountbatten. China, which had been under partial (but expanding) Japanese occupation since the early 1930s, was considered an area in which American operations were to play the leading role.[57] To confuse matters further, American general Joseph Stilwell, who had been dispatched in early 1942 to assist the Nationalist Chinese government of Chiang Kai-shek resist the occupation, was made deputy commander of SEAC under Mountbatten and chief of staff to Chiang.[58] Stilwell had at his disposal only two divisions of poorly trained and unmotivated Chinese troops and a single regiment-size American long-range penetration force, the 5307th Composite Unit, known to history as Merrill's Marauders (named for General Frank D. Merrill).

OSS waded directly into this muddle in mid-1942 and managed to use the dearth of large conventional formations to its advantage by making itself indispensable to Stilwell. At this time, Stilwell had just been forced out of Burma and into India, giving the Japanese control of the Burma Road and limiting the supply line to China to a hazardous air route over the Himalayas. Stilwell was determined to retake Burma but was not remotely interested in employing any irregular methods to do so. He considered guerrilla warfare a form of "illegal action" and insisted on a traditional war of maneuver.[59] Donovan only prevailed on Stilwell to accept a Special Operations Branch element because it was commanded by Major Carl F. Eifler, who Stilwell had known and respected since their service together years prior.[60] Eifler's team, codenamed Detachment 101, set up a base in Nazira, India, just across the border from Burma. After some months of trial and error, Detachment 101 established a highly effective program of infiltration and human-intelligence collection miles behind Japanese lines. By early 1944, when Stilwell was finally ready to initiate his offensive into northern Burma, a Special Operations Branch team that never numbered more than 50 men behind enemy lines had recruited, trained, and equipped some 2,000 anti-Japanese guerrillas from the local Kachin tribesmen.[61] Given the paucity of effective conventional forces at his disposal, Stilwell required Detachment 101's guerrillas to serve as a forward reconnaissance and flank security element.[62] By this time, the detachment had established a strong working relationship with Stilwell, who had neither the time nor the ability to micromanage its operations, meaning that Detachment 101's leaders could employ psychological warfare techniques as they saw fit.

By the time Stilwell's offensive into Burma got underway in early 1944, command relationships in the region had also been clarified—to OSS's benefit. Lord Mountbatten, who took command of the Southeast Asia Command in 1943, was a major proponent of all forms of special operations.[63] Mountbatten was determined to employ special operations units as efficiently as possible in his new command, so upon arrival he established P Division, a division of his staff to consolidate and oversee all special operations and psychological warfare units in the region.[64] P Division was led by an SOE officer with an OSS deputy. The OSS officer chosen was Edmond Taylor, a Morale Operations officer and former journalist who, like Donovan, had directly observed the potency of Nazi propaganda in prewar Europe. He also shared Donovan's views about the need for black propaganda capability to provide direct support to military operations. Taylor played a major role in developing the branch's doctrine. He had served briefly on Eisenhower's Psychological Warfare Board in North Africa, where he saw how the prevailing command relationships resulted in the "complete swallowing up" of Morale Operations Branch functions.[65] His placement as the second in command of P Division proved instrumental in allowing the Morale Operations Branch to play a major role in support of operations in Burma and later in China.

The first Morale Operations officers began arriving in India in mid-1944, when the Burma offensive was well underway. Once in India, they established support offices, developed black propaganda operations, and produced black propaganda materials, including forged orders and letters home from Japanese troops.[66] Though still removed from the front, these officers were able to make an impact in short order by working through intelligence networks that Detachment 101's Kachin guerrillas had established through contacts with fellow tribesmen hired to perform menial tasks in Japanese headquarters facilities. The first such operation came within days of the opening of the Morale Operations office in Delhi. Kachin guerrillas had recovered several bags of mail from Japanese troops waiting to be sent back to Japan. Morale Operations officer Elizabeth P. MacDonald, a former journalist and Japanese linguist who helped establish the Delhi office and who would soon be placed in charge of all Morale Operations in the region, realized that because this mail had already been approved by Japanese military censors, they could change it and have the Kachin intelligence network place it back into the mail system for return to Japan. MacDonald's linguists made subtle changes to hundreds of handwritten letters, reworking the letters so that they made clear the misery and desperation of the Japanese situation, thereby providing an alternative view to the rosy picture of the war that Japanese propagandists fed to their own citizens.[67]

As the war in Burma ground on, MacDonald and her colleagues determined that they could make their greatest contribution by finding a way to counteract the resolve of Japanese troops to fight to the last man rather than surrender. This was a significant issue since Japanese troops were indoctrinated from the moment of enlistment that surrender was the worst possible form of shame, one which also carried stiff legal penalties for the offender and their family. To defeat this deeply ingrained mentality, Morale Operations officers in India drafted a fake order authorizing Japanese troops to surrender if they were hopelessly outnumbered, wounded, sick, or out of ammunition.[68] This order was passed to the first Morale Operations field team specifically organized and equipped to conduct psychological warfare in an austere jungle environment. This four-person team, codenamed Gold Dust, deployed to Detachment 101's forward headquarters in Burma in November 1944. The Gold Dust team brought with it a three-pound portable printing press and other purpose-built production equipment, which allowed it to reproduce the forged order and distribute it widely via the Kachin guerrillas' intelligence network. In at least one case, this was accomplished when a Kachin agent ambushed and killed a Japanese courier on a jungle road, inserted the forged order into the courier's message bag, and then walked to a nearby Japanese headquarters to report finding a dead soldier. This agent led the Japanese to their fallen comrade and stayed with them to observe their surprised reaction to the surrender order.[69] Detachment 101 reported a significant increase in enemy surrenders during the remainder of the Burma campaign.[70]

Morale Operations expanded further still in late 1944 and early 1945 when the Japanese were forced out of Burma and the war moved to China. While operations in China fell outside of SEAC's jurisdiction and thus outside of P Division's authority to coordinate, OSS benefited when General Albert Coady Wedemeyer replaced Stilwell as the commander of the China theater in November 1944. Perhaps uniquely among American theater commanders, Wedemeyer had a strong relationship with OSS for the entirety of the war. Wedemeyer had served on the Joint Psychological Warfare Board, a short-lived War Department effort to oversee psychological warfare operations from Washington before these were assigned to OSS/Morale Operations and OWI sections at each of the theater commands, and he had remained on friendly terms with OSS ever since.[71] Wedemeyer made no effort to change the command relationships that had proven so beneficial to the Morale Operations Branch in Burma, and so the branch's operations in China flourished under Wedemeyer's tenure as theater commander.

From November 1944 to the war's conclusion 10 months later, the Morale Operations Branch deployed some 25 two-person teams into Japanese-occupied China.[72] These teams, embedded among larger Special Operations Branch elements training Chinese guerrillas, deployed with their own mobile production equipment, including three-pound printing presses specially developed for covert propaganda production by highly mobile teams.[73] These teams, and the networks of local agents that they established, were able to distribute material across hundreds of miles of occupied territory.[74] Much of this material was aimed at convincing Chinese troops loyal to the Japanese-sponsored puppet government in Shanghai to defect to the Chinese Nationalists. These efforts were highly effective in inducing Chinese puppet troops to defect, to the point that the Chinese general commanding the Nationalist 34th Army considered the Morale Operations team in Shanxi Province to be more effective in degrading Japanese combat power than all of the Allied bombing campaigns undertaken in the same area.[75] In other cases, their efforts took a more tangible and immediate effect, as when a Morale Operations-induced strike by the rickshaw drivers of Fuzhou paralyzed Japanese troop movements in and around the city just prior to its capture by Nationalist forces.[76] These operations continued right up until the Japanese surrender following the dropping of the atomic bombs on Japan in August 1945. By the end of the war, the teams had collectively distributed millions of pieces of propaganda reaching the entirety of occupied China, from Hong Kong in the south to Shenyang in the northeast, significantly weakening the Japanese hold on mainland China.[77]

Conclusion

Psychological and unconventional warfare are inherently complementary functions in that they aim to undermine enemy strength (both mental and physical) from within. Among the lessons learned from the Morale Operations Branch experience is that psychological messaging is most effective when distributed by human sources (such as those recruited by their Special Operations Branch counterparts) rather than by remote delivery such as radio and air-dropped leaflet or, in more modern contexts, social media. There is no denying that these technologies can reach vastly larger audiences far more quickly than messages disseminated by people, but the message's credibility can be greatly enhanced if it is delivered by a human agent who appears to be a member of the target audience's own side. Indeed, in the contemporary operating context, Russian disinformation agents seem to have learned this lesson and are laundering their deceptive messaging through legitimate media sources rather than simply disseminating it far and wide through fake online personas as they did in 2016.[78]

Another key lesson is the importance of hiring the right skill sets for psychological warfare (including versatility with languages, written and verbal communication, and an understanding of the target audiences' culture and mindset) and allowing the people who possess these skills sufficient latitude to employ them creatively. Barbara Lauwers, Betty MacDonald, and Edmond Taylor, the Morale Operations officers mentioned above, all had previously worked as journalists—backgrounds that gave them experience not only in developing sources and communicating clearly to a target audience but also in operating independently in sometimes austere environments. They also had a certain degree of what one might, for lack of a better term, call guile or cunning: a creative and imaginative streak that allowed them to dream up devious techniques for deceiving the enemy about the plans and intentions of their own superiors. This differed significantly from the PWD approach, which consisted of trying to convince troops, many of whom had already demonstrated a willingness to fight to the end rather than surrender. OSS's approach gave Lauwers and MacDonald wide latitude to employ these skills as they saw fit. As the preceding sections have shown, conventional leadership decisions could be decisive in enabling this approach or in fatally undermining it.

This, indeed, is the most important lesson from the Morale Operation Branch's experience across the three theaters in which it operated. Conventional theater commanders can have a decisive impact on the scope and quality of psychological and unconventional warfare efforts taking place within their areas of operations. When these commanders employed organizational models that allowed for smooth coordination between the elements pursuing these functions, as was the case in the Mediterranean and CBI theaters, they made a significant contribution to the success of the entire campaign. However, traditional military thinking that prizes decisive victory through lethal action can result in organizational decisions that sever the psychological warfare function from its unconventional warfare counterpart, severely limiting its utility. This demonstrates the imperative of having theater commanders who are well trained in the utility of subversive warfare functions and understand that they work best when employed in a complementary manner, rather than viewing information as a nonlethal form of indirect fire that can be disassociated from unconventional warfare activities.

Recent statements by senior U.S. Army officers from the conventional and special operations communities suggest that these lessons have been absorbed by some elements of the Service but not by others. Conversely, U.S. Army special operations units are producing forward-looking strategic documents that suggest they understand these issues and are prioritizing the role of psychological effects in future operations. For example, the Army's 1st Special Forces Command (Airborne), which oversees all of the Army's special warfare functions (including the Civil Affairs, Psychological Operations, and Special Forces Groups) recently produced a future strategy document entitled *A Vision for 2021 and Beyond.* This document makes clear that psychological operations and other nonlethal techniques to influence target audiences in sensitive operating environments will enjoy conceptual parity with the lethal capabilities of the command's Special Forces Groups.[79] It goes on to say that these functions are to be employed in a cohesive fashion by cross-functional teams in a manner similar to Lord Mountbatten's P Division described earlier. The document includes a fictional vignette to illustrate how the concepts it describes might be used to counter Chinese influence in Africa. In this short story, it is the Psychological Operations and Civil Affairs units that play a decisive role through their ability to influence local stakeholders, and the Special Forces Detachment supports them by providing nonviolent support to local protests.[80] All objectives are accomplished by engaging with and leveraging key stakeholders and without resort to lethal action.

This stands in contrast with the efforts of U.S. Army Cyber Command

(ARCYBER), which is currently seeking to rename itself U.S. Army Information Warfare Command and to take responsibility for not only cyber operations but also space operations, electronic warfare, psychological operations, and public affairs.[81] The argument for this expanded mission is that because so much of the information that could impact an adversary's decisions is carried over digital platforms susceptible to cyber or electromagnetic interference that a cyber command is best positioned to conduct information operations over those systems. In comments to the C4ISRNET, a technology-oriented defense news site, the ARCYBER commanding general, Lieutenant General Stephen G. Fogarty said that

> It's more frequent that we will have task to conduct a cyberspace effects operation to generate an [information operations] IO effect. Or we're going to deliver IO content. We're bowing to the reality that offensively, this is what commanders in many cases want us to do for them.[82]

However, it does not follow that because information is carried to human recipients over technical systems, that the best organizations and doctrines for conducting information warfare are those originating in technical disciplines. As Dr. Herb Lin, a cyber warfare expert at Stanford University noted:

> The strongly technical emphasis and history of the DoD cyber warfare community cause me to question whether DoD is well-positioned to embrace and integrate the psychological aspects of information operations. Various service cyber commands (including USCYBERCOM) have concentrated on acquiring the technical expertise that cyberspace operations require. This focus has been entirely proper given their missions to date, but the expertise needed to conduct psychological operations goes beyond the skill set of cyber operators.[83]

In a similar vein, retired Lieutenant General Charles T. Cleveland, who was from 2012 to 2015 the commander of U.S. Army Special Operations Command, recently noted that the military conceptualizes and is organized around warfare in specific domains (air, land, sea, cyber), but that outside of the special operations community, it lacks an adequate appreciation of the human domain in which key audiences are influenced.[84] Without such an appreciation, U.S. military operations will continue to push direct, technical, and often lethal solutions to intractable human problems, which will only serve to extend the frustrations faced by American forces during the wars in Iraq and Afghanistan during the course of the past two decades.

Commanders must understand that information warfare is a fundamentally interpersonal rather than technical endeavor, regardless of whether the message is carried over technical means. It requires a deep understanding of the culture and psychology of the target audience, which can only be achieved when Psychological Operations troops leverage the persistent presence and trust-building engagement efforts employed by units operating in the human domain, such as Civil Affairs and Special Forces Groups, combat advisory units, and the military diplomats resident in the defense attaché offices and security cooperation organizations at nearly every U.S. embassy. Grouping information warfare with the more technical disciplines of cyber and electronic warfare risks repeating the experience of Morale Operations/London, in which the creative propaganda efforts seen in other theaters were paralyzed by their placement under a command accustomed to thinking in terms of immediate, direct effects against enemy units.

Endnotes

1. Operation Jedburgh is the most famous OSS operation of the war and is the subject of at least four historical works: Colin Beavan, *Operation Jedburgh: D-Day and America's First Shadow War* (2006); Will Irwin, *Abundance of Valor: Resistance, Survival, and Liberation: 1944–45* (2010); Will Irwin, *The Jedburghs: The Secret History of the Allied Special Forces, France 1944* (2005); and Benjamin F. Jones, *Eisenhower's Guerrillas: The Jedburghs, the Maquis, and the Liberation of France* (2016). It is also the subject of two separate chapters in a recent Army study on special operations in major war. See Robert M. Toguchi and Michael E. Krivdo, eds., *The Competitive Advantage: Special Operations in Large-Scale Combat Operations* (Fort Leavenworth, KS: Army University Press, 2019).
2. As of this writing, only historian Clayton D. Laurie has written on the Morale Operations Branch, but his work focuses on its founding and bureaucratic battles with other elements of the U.S. government's wartime propaganda apparatus; the branch's activities form a very minor part of his account. There is not yet a comprehensive history of the Morale Operation Branch's operations in the field. See Clayton D. Laurie, *The Propaganda Warriors: America's Crusade Against Nazi Germany* (Lawrence: University Press of Kansas, 1996).
3. I. C. B. Dear and M. R. D. Foot, eds., *The Oxford Companion to World War II* (Oxford, UK: Oxford University Press, 1995), https://doi.org/10.1093/acref/9780198604464.001.0001. Terminology for these types of operations has changed significantly in the decades since World War II. In OSS documents, the term *special operations* referred narrowly to the provision of weapons and training to resistance groups behind enemy lines, or what is now known in U.S. doctrine as "unconventional warfare."
4. Laurie, *The Propaganda Warriors*, 134.
5. Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder* (New York: William Morrow, 2019), 109–10.
6. Ben Connable, Jason H. Campbell, and Dan Madden, *Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War* (Santa Monica, CA: Rand, 2016), https://doi.org/10.7249/RR1003.
7. Eric Robinson, "The Missing, Irregular Half of Great Power Competition," Modern War Institute at West Point, 8 September 2020.
8. Douglas Waller, *Wild Bill Donovan: The Spymaster Who Created the OSS and Modern American Espionage* (New York: Free Press, 2011), 50–55.

9. Col William Donovan and Edgar Mowrer, *Fifth Column Lessons for America* (Washington, DC: American Council on Public Affairs, 1941), 8.
10. OSS historian Bradley F. Smith saw Donovan's fears of fascist propaganda as wildly exaggerated. Bradley F. Smith, *The Shadow Warriors: O.S.S. and the Origins of the C.I.A.* (New York: Basic Books, 1983), 417.
11. Kermit Roosevelt, *War Report of the OSS (Office of Strategic Services)*, vol. 1 (New York: Walker, 1976). Original classified edition published by the Strategic Services Unit of the U.S. War Department, 1946, 29–82.
12. Edmond Taylor, *Awakening from History* (Boston, MA: Gambit, 1969), 309.
13. Laurie, *The Propaganda Warriors*, 93.
14. Alfred H. Paddock *U.S. Army Special Warfare: Its Origins*, rev. ed. (Lawrence: University Press of Kansas, 2002).
15. Roosevelt, *War Report of the OSS*, vol. 1, 21.
16. *Morale Operations Field Manual—Strategic Services (Provisional)* (Washington, DC: Office of Strategic Services, 1943). Digital declassified copies of OSS field manuals have been produced by the U.S. Army Special Operations Command and are available online.
17. David W. Hogan Jr., *U.S. Army Special Operations in World War II* (Washington, DC: U.S. Army Center of Military History, 1992), locs. 436–48 of 6884, Kindle.
18. Hogan, *U.S. Army Special Operations in World War II*, loc. 454 of 6884.
19. David E. Johnson, *Fast Tanks and Heavy Bombers: Innovation in the U.S. Army, 1917–1945* (Ithaca, NY: Cornell University Press, 1998), 68.
20. Paddock, *U.S. Army Special Warfare*, 18.
21. Quoted in Michael R. Matheny, *Carrying the War to the Enemy: American Operational Art to 1945* (Norman: University of Oklahoma Press, 2011), 53.
22. Matheny, *Carrying the War to the Enemy*, 53.
23. Milton E. Miles, *A Different Kind of War: The Little-known Story of the Combined Guerrilla Forces Created in China by the U.S. Navy and the Chinese During World War II* (New York: Doubleday, 1967), 86.
24. Miles, *A Different Kind of War*, 123.
25. Clayton D. Laurie, "General MacArthur and the OSS, 1942–1945," *Studies in Intelligence* (September 2014).
26. Leachman's exploits are detailed in N. N. E. Bray, *A Paladin of Arabia: The Biography of Brevet Lieut.-Colonel G.E. Leachman, C.I.E., D.S.O., of the Royal Sussex Regiment* (London: Unicorn Press, 1936); and Shakespear's activities are related in H. V. F. Winstone, *Captain Shakespear: A Portrait* (London: Jonathan Cape, 1976).
27. A. R. B. Linderman, *Rediscovering Irregular Warfare: Colin Gubbins and the Origins of Britain's Special Operations Executive* (Norman: University of Oklahoma Press, 2016), 37.
28. M. R. D. Foot, *SOE: The Special Operations Executive 1940–46* (London: British Broadcasting Corporation, 1984), 20–21.
29. Linderman, *Rediscovering Irregular Warfare*, 100.
30. Charles Cruickshank, *The Fourth Arm: Psychological Warfare, 1938–1945* (London: Davis-Poynter, 1977), 31.
31. Cruickshank, *The Fourth Arm*, 43.
32. Paddock, *U.S. Army Special Warfare*, 11.
33. Paddock, *U.S. Army Special Warfare*, 12.
34. *The Psychological Warfare Division, Supreme Headquarters Allied Expeditionary Force: An Account of Its Operations in the Western European Campaign, 1944–1945* (Washington, DC: War Department, 1945), 8.
35. *The Psychological Warfare Division, Supreme Headquarters Allied Expeditionary Force*, 6.
36. *PWB, Psychological Warfare Branch, Combat Team* (Camp Sharpe, PA: U.S. Army Psychological Warfare Training Center, 1943), 60–61. Digital copy in author's possession.
37. Nelson D. Lankford, ed., *OSS against the Reich: The World War II Diaries of Colonel David K. E. Bruce* (Kent, OH: Kent State University Press, 1991), loc. 1335 of 5734, Kindle.

38. Lankford, *OSS against the Reich*, loc. 1855 of 5734.
39. Lankford, *OSS against the Reich*, loc. 2643 of 5734.
40. Nelson MacPherson, *American Intelligence in War-time London: The Story of the OSS* (London: Frank Cass Publishers, 2004), 205.
41. MacPherson, *American Intelligence in War-time London*, 205.
42. *Report on OSS Morale Operations in the European Theater of Operations* (London: Office of Strategic Services Mission to Great Britain, 1945). Reproduced by PsyWar.org and posted in plain text without pagination directly to the website.
43. *Report on OSS Morale Operations in the European Theater of Operations.*
44. *Report on OSS Morale Operations in the European Theater of Operations.*
45. *Report on OSS Morale Operations in the European Theater of Operations.*
46. *Report on OSS Morale Operations in the European Theater of Operations.*
47. *Report on OSS Morale Operations in the European Theater of Operations.*
48. All three of these units were established in the British Middle East Command during 1941–43, when the situation in the campaign against the German *Afrika Korps* was particularly desperate. After the defeat of German forces in Africa, these units went on to serve throughout the Mediterranean theater, particularly in Yugoslavia and the Dodecanese Islands. See Gavin Mortimer, *The SAS in World War II: An Illustrated History* (Oxford, UK: Osprey Publishing, 2015); Gavin Mortimer, *The SBS in World War II* (Oxford, UK: Osprey Publishing, 2017); and Gavin Mortimer, *The Long Range Desert Group in World War II* (Oxford, UK: Osprey Publishing, 2017).
49. Erasmus H. Kloman, *Assignment Algiers: With the OSS in the Mediterranean Theater* (Annapolis, MD: Naval Institute Press, 2005), 28.
50. Laurie, *The Propaganda Warriors*, 196–98.
51. Laurie, *The Propaganda Warriors*, 198.
52. Elizabeth P. McIntosh, *Sisterhood of Spies: The Women of the OSS* (Annapolis, MD: Naval Institute Press, 1998), 61–62.
53. McIntosh, *Sisterhood of Spies*, 62–65.
54. McIntosh, *Sisterhood of Spies*, 65–66.
55. Reproductions of the original leaflets as well as English translations are available at PsyWar.org.
56. Laurie, *The Propaganda Warriors*, 194.
57. Richard J. Aldrich, *Intelligence and the War against Japan: Britain, America, and the Politics of Secret Service* (Cambridge, UK: Cambridge University Press, 2000), 142.
58. Barbara Tuchman, *Stilwell and the American Experience in China, 1911–1945* (New York: Random House, 1970), loc. 216 of 13561, Kindle.
59. Miles, *A Different Kind of War*, 76.
60. Miles, *A Different Kind of War*, 86.
61. William R. Peers and Dean Brelis, *Behind the Burma Road: The Story of America's Most Successful Guerrilla Force* (Boston, MA: Atlantic Monthly Press, 1963), 139.
62. Peers and Brelis, *Behind the Burma Road*, 162–65.
63. Aldrich, *Intelligence and the War against Japan*, 183.
64. Aldrich, *Intelligence and the War against Japan*, 179.
65. Aldrich, *Intelligence and the War against Japan*, 181.
66. Elizabeth P. MacDonald, *Undercover Girl* (New York: Macmillan, 1947), 73.
67. MacDonald, *Undercover Girl*, 80–82.
68. MacDonald, *Undercover Girl*, 89–90.
69. MacDonald, *Undercover Girl*, 94–97.
70. Peers and Brelis, *Behind the Burma Road*, 181.
71. Maochun Yu, *OSS in China: Prelude to Cold War* (Annapolis, MD: Naval Institute Press, 1996), 171.
72. John W. Brunner, "OSS Teams in China," in *OSS Special Operations in China*, ed. Francis B. Mills, Robert Mills, and John W. Brunner (Williamstown, NJ: Phillips Publications, 2002), 511–13.
73. MacDonald, *Undercover Girl,* 167.
74. MacDonald, *Undercover Girl*, 171.

75. MacDonald, *Undercover Girl*, 216.
76. MacDonald, *Undercover Girl*, 174.
77. For the volume of propaganda produced, see MacDonald, *Undercover Girl*, 201. For the geographic spread of the OSS teams and their agent networks, see "Map: OSS Field Teams and Agent Nets in China," reproduced in Mills, Mills, and Brunner, *Special Operations in China*, 498.
78. Sheera Frenkel and Julian E. Barnes, "Russia Again Targeting Americans with Disinformation, Facebook and Twitter Say," *New York Times*, 1 September 2020.
79. *A Vision for 2021 and Beyond* (Fort Bragg, NC: 1st Special Forces Command [Airborne], U.S. Army Special Operations Command, 2020).
80. *A Vision for 2021 and Beyond*, 13.
81. Mark Pomerleau, "A New Name—and Focus—for Army Cyber Command?," C4ISRNET, 21 August 2019.
82. Pomerleau, "A New Name—and Focus—for Army Cyber Command?"
83. Herb Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD," *Cyber Defense Review* 5, no. 2 (Summer 2020): 101.
84. Charles Cleveland et al., *Military Strategy in the 21st Century: People, Connectivity, and Competition* (Amherst, NY: Cambria Press, 2018), locs. 2982–3005 of 3984, Kindle.

All Women Belong in the Kitchen, and Other Dangerous Tropes

Online Misogyny as a National Security Threat

Kyleanne Hunter, PhD, and Emma Jouenne

Abstract: Online misogyny is an under-studied form of information warfare. Often dismissed as "boys will be boys," online misogyny has been allowed to percolate and create communities that have far-reaching impacts. The impacts of online misogyny are not confined to the internet. In this article, the authors show how the ubiquitous nature of online misogyny poses a national security threat. We explore three diverse case studies: the United States military, the incel movement, and ISIS to demonstrate the far-reaching nature of the security threat. Though the nature of the security threats is different, the intervening cause—unchecked online misogyny—is the same.

Keywords: misogyny, online radicalization, security

In her introduction to *Not All Dead White Men: Classics and Misogyny in the Digital Age*, Donna Zuckerberg describes how the internet, social media in particular, has allowed a previously undefined and disconnected group to congregate and find a home. This group—composed of men focused on what they espouse to be "traditional values"—has collectively created spaces on the internet where online misogyny is allowed to take root and grow a narrative that

Dr. Kyleanne Hunter is an assistant professor of military and strategic studies at the U.S. Air Force Academy in Colorado Springs, a nonresident fellow at the Brute Krulak Center for Innovation and Creativity at Marine Corps University, and a senior adjunct fellow at the Center for a New American Security. She is a Marine Corps combat veteran and former chair of the Employment and Integration Subcommittee of the Defense Advisory Committee on Women in the Services. The views presented are her own and do not represent her employer or the Department of Defense. Emma Jouenne is an MA candidate in security studies at Georgetown University. She is the associate editor for gender and international relations at the *Georgetown Security Studies Review*.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201003

men are being threatened by an ever-modernizing and diverse society. These online communities are not solely a place where frustrated men go to speak ill about women. We find that they produce a politically charged form of information warfare that has consequences to the United States' security. Recent events have shown just how close to home these threats are. On 6 January 2021, an angry mob of mostly male rioters stormed the United States Capitol Building. While their attacks were politically motivated, the rioters displayed aspects of violent misogyny. From donning military attire to literally thumping bare chests to breaking into Speaker Nancy Pelosi's office and putting their feet on her desk, the rioters—most of whom were radicalized online—gave us an upfront view of what violent manifestations of misogyny actually look like.[1]

Zuckerberg's account of how misogyny has found such a stronghold in online communities is reminiscent of Cynthia Enloe's simple question 30 years ago: "where are the women?"[2] While the internet and social media have allowed for advancements in communication, economics, and education, it has also emboldened and elevated vitriolic forms of misogyny. As Alice Marwick and Rebecca Lewis note, online chatrooms, forums, and social media platforms are the primary means of communication for communities or groups espousing misogynistic beliefs, and the online environment has allowed for the cross-pollination of ideas between geographically distant and culturally diverse individuals and organizations.[3] Yet, this part of the internet is rarely talked about, especially in the traditional security sector. In their introduction to a special edition of *Feminist Media Studies* on online misogyny, Debbie Ging and Eugenia Siapera discuss how women's experiences online are most often treated as personal matters that government responses have no place in addressing and fall short of warranting a place in public security discourse.[4] The dismissal of women's concerns comes despite both scholars and victim advocates raising concerns about the degree to which online threats need to be taken seriously and the particularly unique nature of social media to breed "cyber mobs."[5] Victims often find themselves in a double bind—where legally they are at odds with speech protected by the First Amendment while also being socially isolated based on the nature of how they were harassed or attacked.

The categorizing of women's experiences online as private should not come as a surprise. Traditional military and security studies are focused primarily on safety of the state by external threats. Women's security concerns have been historically absent from the traditional security apparatus, treated as private issues to be dealt with once "real security" is handled.[6] In the physical world, this results in ill consequences ranging from women servicemembers being more susceptible to musculoskeletal injuries due to ill-fitting uniforms and equipment to the underreporting of rape.[7] The historic absence of women in the security sector does not just harm women. It has also made the conduct of war more difficult, especially in culturally sensitive contexts such as counterinsurgency operations.[8] Feminist scholarship has pushed to begin a meaningful dialogue about the importance of gender equality and gendered security, yet it remains largely absent in conversations of online security, information warfare, or digital propaganda. This has allowed online misogyny to evolve unchecked.[9]

We find that advancements in digital communications have allowed for beliefs held by physically dispersed individuals to coalesce, and the consequences of their beliefs are seen in internal and external security threats. Internally, the unchecked proliferation of misogyny, including among members of the Armed Services, has resulted in a reduction in propensity to serve among young American women, a population critical to the Services reaching their needed force strength and necessary for the conduct of culturally sensitive operations at home and abroad. Externally, gendered online propaganda and targeted "manosphere" discussions are used to recruit violent extremists and create a sense that they are fighting for virtue and values.[10] These twin threats both pose physical security risks and also undermine the United States' foundational values of civil and individual liberties. Online misogyny must be considered information warfare because it both disrupts and undermines democratic values and has consequences in the real world.[11] In this article, we use a most different research design with the cases of the United States military, the incel movement, and the Islamic State in Iraq and Syria (ISIS) to show the breadth of the security threat posed by online misogyny.[12] The article's discussion shows how these threats are linked by the pervasiveness of online misogyny, and it provides recommendations for how the U.S. government, the relevant security institutions, and the private sector should address this phenomenon.

Background: Online Misogyny as Information Warfare

Misogyny is often trivialized as simply disliking women. But as Kate Manne notes, its roots are much deeper; it is "a political phenomenon whose purpose is to police and enforce women's subordination and to uphold male dominance."[13] It focuses on structurally ordering society in such a way that women are degraded, undermined, and denied access to equal rights. In extreme cases, it results in women facing hostile consequences if they violate the norms associated with their role. The strain of misogyny most often found in the online environment is rooted in a belief that society is experiencing a "decline of males" as a response to the increased presence of women in the labor force and sociopolitical positions of power.[14] Domestically, the loose and diverse collection of men's rights activists adhering to this ideology has become known as the "manosphere."[15] However, online misogyny transcends the manosphere. Hidden in benign and benevolent sexism, adherence to professed traditional values and beliefs about social protection, online misogyny's impacts are diverse.[16]

A review of the literature shows two particularly dangerous aspects of online misogyny. First, the specific type of masculinity espoused in this propaganda is strongly linked to violence. The communal and connected nature of the online environment creates a space where individuals holding these beliefs convene, often leading to action in the real world. Second is the ability to propagate falsehood and pseudoscience in a continual and factual seeming manner. The platforms used to spread misinformation provide a sense of legitimacy. Taken together, they present a unique form of information warfare that poses a security threat to the United States.

Violent Roots of Hegemonic Masculinity

Online misogyny communities are a particularly dangerous manifestation of information warfare because of how closely the form of masculinity practiced in these circles is linked to violence. Their beliefs on masculinity center on toughness, strength, power, and dominance and espouse a hierarchical ordering principle that views women as "less than" due to a rigid "gender system."[17] This ideology creates rules of distinctive separation linked to beliefs about masculine and feminine norms, and it attributes higher value to things perceived as masculine. Men and women have distinct roles and places in societies, and it is a man's duty to engage in violence to preserve that order. It is important to note that gender norms and practices differ based on cultural differences.[18] However, the hierarchical gender system that results in violence is a constant across cultures. Though this belief system is often espoused through the language of honor—men being "just warriors" to protect women's "beautiful souls"—it is often manifested through less-than-honorable violence.[19] This is exemplified in M. Christina Santana et al.'s finding that men who reported adhering to these traditional beliefs about masculinity engaged in sexual and intimate partner violence significantly more than those who did not.[20] Belief in men's dominance over women is also correlated with participation in larger-scale political violence.[21] Strong adherence to patriarchal values coupled with a belief that men are "tougher" than women creates what Karen Brounéus, Elin Bjarnegård, and Erik Melander describe as an "honor ideology."[22] Men who subscribe to this ideology are more likely to engage in violence specifically to counter gender equality norms and policies. Joshua M. Roose further expands on this linkage. He finds this ideology leads to beliefs that women's empowerment has left men victimized and discriminated against. They play out their anger and resentment through violent acts, justifying them as merely reclaiming the power they believe is rightfully theirs.[23] Online, men go to great lengths to create a persona steeped in the trappings of their views on masculinity. In analyzing identity performance in this space, Joseph A. Vandello et al. finds that there is a certain "precarious manhood" that is overacted when there is a perceived threat from advancements in women's rights or social position.[24] The degree to which violence—or speech inciting violence—is a result of this practice is proportional to the threat that men feel.[25] The more that men are pushed to believe that women are threatening what they view to be the "natural order," the more accentuated their violent reactions will be.

While individuals holding such beliefs are harmful to those in their immediate surroundings, the internet magnifies and accelerates these feelings, amplifying the damage that can be done. The internet is adept at facilitating political assemblages that unite around emotional involvement and ideals.[26] As Laura Bates notes, the internet adds a layer of social interaction to the users' experience and reinforces the density of their relationships.[27] It continues to move misogyny from a fringe idea to a ubiquitous feature of the online environment. During the past two decades, we have seen an uptick in radicalized violent organizations, hate groups, and other forms of misogyny on diverse social media platforms. Easy access to technology has increased misogynistic radicalization at a pace with which neither the security sector nor the law has kept up. The widespread recruitment that the virtual world has facilitated has moved misogyny into the information warfare domain.[28] There is a lack of preparedness and coordination among government and private security agencies to mount an appropriate and proportionate response to this new threat. This protean threat is evolving in two related "war zones" with shifting and ill-defined borders: cyberspace and the information space.

The Firehose of Falsehood

As the recent Capitol attacks on 6 January 2021 and President Donald J. Trump's second impeachment show, information is a political tool that encourages violence. Such violence inciting rhetoric is an example of Christopher Whyte's view of information warfare as a tool that threatens security through its disruption and undermining of democratic processes and values.[29] The threat posed not only harms women, but as will be shown, undermines the very foundations of the United States' principles. The threat posed by online misogyny is bolstered through the use of language. Online misogyny adheres to what has been dubbed the "firehose of falsehood" approach to disinformation propaganda, where lies are told often and confidently enough that they become adopted as truths.[30] The increased customization and specificity of individuals' online experience helps to accelerate the firehose of falsehood effect. As social media, search engines, and online chat communities work to personalize the experience for users, online echo chambers are created that reinforce false narratives to the point that they are accepted as truth.[31] This phenomenon is accelerated when information comes from official-sounding sources. Soroush Vosoughi, Deb Roy, and Sinan Aral found that false information spreads faster and is more quickly believed than truthful information online due to both the novelty of the information and the feelings of connection to the source.[32]

To strengthen the firehose of falsehood, official sources are often cited and are distorted to meet a false narrative. This is seen in examples such as the use of a discredited interpretation of the Pareto Principle arguing "20% of men get 80% of women" to general officers asserting that women are too delicate to be a part of infantry units.[33] In surveying the top four studies of actual fake news in the United States, John Corner finds that in the majority of instances, fake stories cite an official data source or official agency to attempt to lend credibility to their claims.[34] Yet in asserting their claims, the data is taken largely out of context or misused. An example of this is the use of a Centers for Disease Control and Prevention (CDC) national prevalence survey on intimate partner violence on incels.co to assert that "men are more likely to suffer intimate physical violence than women."[35]

Manipulation of official-sounding data serves to embolden misogynistic beliefs and recruit dissatisfied individuals. The official-sounding narrative allows for unfounded information to appear more truthful. The type of disinformation contained in the firehose of falsehood paints women as both victims (i.e., losing their real womanhood to overly feminist Western society) as well as perpetrators (i.e., responsible for the spread of COVID-19 or the loss of military effectiveness). This dual narrative results in a compounded negative view of women. Social media has created a platform that has given these views a sense of legitimacy and fueled public debate.[36] This gendered disinformation creates a security threat through both pushing women out of the formal security sector and providing justification for violence against those who hold values of egalitarianism.

Methods and Hypotheses

We use a most different research design to show the far-reaching and diverse impact that online misogyny has on national security. The United States military, the incel movement, and ISIS are diverse organizations, with missions, ideology, and in-group practices that differ greatly. ISIS represents a direct threat to the physical security of U.S. interests while the incel movement undermines democratic norms and values of equality, and the military is responsible for protecting U.S. national security. They do, however, have similarities. They are male dominated and have historical anti-women biases that are both formal (i.e., legal restrictions on the jobs women in the military are able to hold) and informal (i.e., biases against women being in nontraditional roles). Yet, one similarity is striking—they all rely on the online environment as a primary communication tool, making them susceptible to online misogyny. The experienced consequences of online misogyny represent the varied ways in which information warfare harms U.S. security. The case of the military represents a threat via omission. It shows how misogynistic speech and propaganda harms the United States through excluding or omitting certain groups from the security sector. This omission makes it easier for violence to be enacted against the continually underrepresented group. The continued cycle of rhetoric and abuse has left the United States in a vulnerable position. The incel movement and ISIS represent threats through commission. Misogynic rhetoric incites individuals to engage in violence in a way they would not absent the gendered rhetoric. Though the types of security threats appear dissimilar, it is important to study them collectively because the driver of the security threat is the same—and mutually reinforcing. The gendered rhetoric used to incite violence has largely slipped through the cracks of the traditional security apparatus, making the United States and its interests susceptible to attacks. However, the diverse perspectives needed to address this security concern are being pushed out by the very same phenomenon. We need more women's perspectives in security to fully address the gendered nature of violent extremism, yet online misogyny is pushing them out of the security sector. While anti-women sentiments have existed long before the internet, the online environment has accelerated its spread and helped to grow its reach.

Using a most different research design in this case shows how sizable of an impact online misogyny has on security. As Carsten Anckar notes, most different designs are beneficial for isolating phenomena that interact with diverse systems in potentially different ways but ultimately have a common outcome.[37] The ubiquitous nature of online misogyny is such a phenomenon. It is not limited to one group. A survey of U.S. social media posts found that more than one-half contained misogynistic content, even if not explicitly part of an explicit anti-woman group.[38] A most different design is also important for identifying a set of solutions that can impact multiple problems simultaneously. As the article will show, policy and practice interventions that address the dangers posed by the manosphere have impacts that address multiple security concerns. Such interventions are not only resource efficient but also address a root cause, leading to more lasting change.

We tested two hypotheses to determine the relationship between online misogyny and national security.

H1: *Online misogyny makes recruiting into the military more difficult*

H2: *Online misogyny intensifies violent tendencies of radical groups*

H1 tests the internal security threat that online misogyny poses. Recruiting women is vital for national security, both to meet needed recruiting numbers and to ensure the military has access to the skills it needs for current and future conflicts.[39] If this hypothesis holds, we will see a reduction in women's propensity to serve and/or a higher rate of attrition for women once they join the Service as a result of online misogyny. H2 tests the external security threat of online misogyny. The strong link between hegemonic masculinity and violence leads to physical insecurity for the United States and its interests abroad. If this hypothesis holds, we will see an uptick in violent attacks as a result of online misogyny.

Research to test H1 was conducted through focus groups of active duty military servicemembers. Focus groups were conducted between 2015 and 2019 during one author's tenure on the Defense Advisory Committee on Women in the Services. They were conducted each spring on bases representing all five Services (Navy, Marine Corps, Army, Air Force, and Coast Guard). Participants were divided by rank (junior enlisted, senior enlisted, and officer) and gender to create an environment that was conducive to free and honest discussion. Focus group protocols were grouped into three main categories: propensity to serve, recruitment and retention, and beliefs about belonging. Each focus group was also given a miniature survey to capture demographic information, including years of service and plans for retirement/separation. All data collection instruments were ruled exempt by ICF's institutional review board with concurrence from the Department of Defense's Office of the Undersecretary of Defense for Personnel and Readiness to ensure protection of human subjects. Focus groups were transcribed by a contracted ICF research team. Analysis of transcribed focus groups was undertaken by a diverse team without existing conflicts of interest. Content review was done during a period of four weeks with weekly meetings for discussion of leading emergent themes and to ensure inter-rater reliability. A total of 2,834 individuals participated in focus groups. The gender breakdown was 44 percent identifying as women, 52 percent identifying as male, and 4 percent declining to identify. Thirty-two percent of participants were officers and 68 percent enlisted. Women and officers were oversampled to ensure diversity in opinions. H2 was tested through discourse analysis of posts by ISIS and the incel movement. Discourse actively constructs the social world. Discourse analysis allows us to gain insight into social interaction and motivation for action, as discourse creates a world that appears as real or true for the writer as the physical world around them.[40] The authors coded posts from incels.co, from March–June 2020. The incels.co forum is host to more than 12,000 members. We analyzed a 500-message sample, representing a cross-sample of key subforums on incel.co. The keywords "women," "femoids," "foids," "deserve," "die," and "violence" were evaluated for frequency and nature of occurrence. We also coded the interrogation of Alek Minassian, perpetrator of an attack in Toronto, Canada.[41] This provided the authors with insight into slurs or speech that were not explicitly violent yet signaled violent intent.

Additionally, we coded articles from three newspapers: *Al-Naba*, *Dabiq*, and *Al-Rumiyah* from 2014 to 2020. These outlets were chosen based on the size of their readership, the frequency of publication, and their role as recruitment tools by ISIS. *Al-Naba* is a weekly newspaper published since 2014 by ISIS. *Dabiq* is an online magazine, which ran from 2014 to 2016. *Al-Rumiyah* replaced *Dabiq* in September 2016. They serve as the primary recruitment tool for new members. The articles extracted from those outlets are therefore assumed to be representative for propaganda contents of the Islamic State and serve as appropriate objects for the analysis. Articles were coded for gender roles (how men and women were portrayed), incentives for committing violence, and descriptions of those who engaged in violence.

Findings

Testing H1—The Internal Threat: Shutting Women out of Security

The relationship between misogyny and the U.S. military is not a new development. The military has and continues to be criticized as an overly white, male institution whereby both through commission and omission women have been marginalized.[42] However, prior to the advent of the internet, the impact of misogyny was more limited. The prevalence of the online environment has accelerated and elevated the impact of misogyny. The direct impacts of institutional misogyny have been persistent and violent. From the Tailhook scandal to the murder of Army Specialist Vanessa Guillen, women within the military have directly suffered the results of institutional misogyny.

While the existence of misogynistic expressions as part of military culture are nothing new, the online environment is leading to new expressions and more far-reaching impacts. No longer confined to the barracks or isolated events, young recruits (or potential recruits) are being exposed to these sentiments earlier and more frequently. The nature and degree of exposure has resulted in different types of outcomes. In addition to the direct threat to women, there is also an impact on propensity to serve. Social media is a primary medium used by young people to gain information about their future careers.[43] Even beyond career searching, American teens spend approximately nine hours per day consuming digital media.[44] Given the prevalence of digital communication to youth, it is nearly impossible for them not to engage with some form of misogyny online. The result is a reduction in the talent pool from which the military can draw.

Analysis of focus group transcripts finds support for H1: online misogyny was a key factor in women's decision to either not join or to leave the military. We found two primary causal pathways linking online misogyny to military recruitment and retention challenges. First, there were direct misogynistic attacks from male servicemembers against their female counterparts. These attacks were often perpetuated by male members of women's units and led to hostile workplaces and reduced retention. Second, there were generalizations made by military groups or pages online about the character and necessity of women's service in the military. Though less targeted, the nature of the messenger in these instances elevated the impact of this pathway.

Personal Attacks from Unit Members

Like all Americans, servicemembers often use social media to share their personal life, posting photos from vacations and celebrating life's accomplishments. Many focus group participants discussed how social media is the primary way to stay in touch with physically distant friends and family. However, it has also become a means by which women are being harassed and targeted. Most commonly, servicemembers described social media as a medium by which senior men were able to harass more junior women. As one junior enlisted member noted:

> You can't say no to their friend request because you don't know if this is an official request or something else.[45]

Most junior women in focus groups expressed being uncomfortable with at least some of the comments that their senior male "friends" made on their posts or comments. Another junior enlisted woman noted:

> It made me uncomfortable the way he was always talking about my body . . . sexualizing it, talking about the things he liked . . . all of a sudden I was no longer a [servicemember] but a piece of meat.[46]

Women reported feeling uncomfortable or unable to report these issues, since the perpetrator of the harassment was often in their direct chain of command. The net result is women leaving the Service due to a feeling a lack of belonging and a lack of belief that their concerns will be adequately addressed. In the miniature survey accompanying focus groups, women outpaced men nearly 2:1 in saying they were planning on leaving the Service as soon as they were eligible for separation. The disparity was even greater for officers, with only 15 percent of women saying they had plans to stay in past their initial obligation, compared to 62 percent of men. The majority of servicemembers participating in focus groups cited the discomfort they felt online as a primary factor in their decision to leave the Service.

Personal online attacks were not isolated to social media "friends." Women often reported that photographs of them from official events—whether their personal command image or official pictures from unit functions—were used maliciously in the creation of memes and shared online. The rhetoric used in these memes discussed rape and murder, evidence of the link between the type of masculinity performed by individuals engaged in online misogyny and the potential for violence. This rhetoric has intensified as more women have entered the Services. It is likely that women in the military are experiencing a backlash in response to their perceived challenge to the masculine status quo.[47] The most prominent instance of this was the Marines United scandal.[48] Though Marines United received prominent media coverage, this phenomenon was widespread. Several woman officers who participated in the focus groups reported having had at least one official photograph taken and turned into a meme. It is important to note that these social media posts persist despite the Services having guidelines for all unofficial postings. For example, Marine Corps guidelines include content that "is defamatory, threatening, harassing, or which discriminates based on a person's race, color, sex, gender, age, religion, national origin, sexual orientation or other protected criteria" as punishable under Article 92 of the Uniform Code of Military Justice (UCMJ).[49] That such posts continue suggests that individuals believe that the guidance is unenforceable, or that leadership does not care to address it.

The fear of continued attacks on social media has negative impacts on women's propensity to serve. As one female officer noted:

> The recent Marines United scandal . . . was very discouraging. . . . If I was thinking of joining, I would maybe look at something else.[50]

Women servicemembers saw this as not only impacting them but the future of the Service. In discussing her experiences with being attacked online, a female officer noted:

> For me it is too late, but that sexual stuff is everywhere. I would not let my daughter join with all that.[51]

The military relies heavily on currently serving members for recruitment. In 2019, 80 percent of new enlistees had a family member who had served in the military.[52] Online misogyny is not only harming the current force, but it has the potential to harm the force for generations to come.

How Military Social Media Pages Represent Women

Focus groups almost unanimously noted that social media was a means by which the Services could—and should—share official information with their members as well as communicate with the public about military life. More than 66 percent of new recruits cite the Services' social media as a primary source of information they referenced prior to going to their initial training.[53] The increased prevalence of official command social media pages is a clear attempt by the Services to speak directly to the younger generation in the way that is most effective for them. The official nature of these pages exemplifies the impact of an official messenger perpetuating damaging information. From the official Marine Corps' Instagram page posting "Saturday Is for the Boys" under a picture of infantry Marines, to the Army having less than 1 percent women represented in official social media, the notion that men are the ideal warfighter continues to be perpetuated by official sources.[54]

The consequences of this can be seen in women's beliefs about their service. When asked directly about their feelings on service and the pathway to serving, most women participating in focus groups indicated that the representation of service women on social media *discouraged* them from serving. As one enlisted woman noted:

> As females, we are doubted immediately. For males, it is "At least you tried." For females . . . the way they represent us we know we are going to be doubted up front [when joining]. Most people just don't want that.[55]

For those who chose to serve despite feelings that they did not belong, the majority felt dissuaded from serving in combat arms jobs because the Service had portrayed them as belonging exclusively to men. As a senior enlisted woman noted:

> I went back home as a recruiter's assistant. . . . There was a girl who wanted nothing more than to be in a [combat occupational specialty]. I heard [the stereotype] echoed by the recruiter. He [said], "Do you know what this is going to entail?" He was doubting her mental strength. Echoing what he heard about women not being able to do the job.[56]

Many servicemembers feel that there is no way that this can be overcome by current leadership. As one officer stated:

> It's crazy. . . . You get [online and see inappropriate posts] on [my Service's] Facebook page, and what can you do about it because every day it's something new, and in the comments people feel like they have the rights to express all their nasty feelings . . . [these pages] have propped up people who feel the need to express everything before they think about it and don't realize how many women see what they post.[57]

Social media was also largely responsible for misinformation being spread about women's ability to meet physical standards for service in combat arms roles and the impact that women were having on the effectiveness of these units. When asked directly about their biggest concerns, most male servicemembers responded that they believed that standards were being lowered to accommodate a "social justice" agenda at the expense of military effectiveness. But when asked why, none could point to an official source. One junior enlisted man noted:

> I read that on the military.com source. But I haven't heard anything else more reputable. I haven't heard commanders say anything, so I believe military.com.[58]

A senior enlisted man noted:

> I've seen more articles from Facebook about what's going on in [my Service] than from my own command.[59]

Women servicemembers recount the impact that the perpetuation of social media misinformation has on their careers. One junior enlisted woman in a ground combat specialty noted:

> When we were integrating, they were like, "Standards are going to go low," and I've heard men in our unit talk about [physical fitness] standards, and they are jealous, like, "The females have low standards and I want that." It's just too much. They don't trust me and there is no way I can get them to believe I am doing the same work as them.

Despite all occupational specialties being open to women, and the Services creating gender integration implementation plans to recruit and retain more women, online misogyny is harming the ability of the Services to recruit and retain this needed demographic. Women remain less than half as likely to join the military as men, and when they do join are 28 percent more likely to leave the Service and are promoted at lower rates than their male counterparts.[60]

Testing H2—The External Threat: Online Misogyny to Promote Violence

A focused backlash against "modernization" is increasingly being used by violent extremists.[61] A particular aspect of modernization that these groups target is the increased role of women in sociopolitical life. They cast feminism and the Western lifestyle as the enemy to promote the use of violence. Traditional gender norms create a very simple frame through which to view the world, and the online environment allows for the amplification of ideology that leads to violence.

To test H2, we analyzed the rhetoric of the incel movement and ISIS. We find support for online misogyny intensifying the likelihood of violent attacks by these groups. This is seen through two primary mechanisms. First, the online environment intensifies individual feelings of resentment over what they believe is lost power and provides an impetus for collective violence. And second, there is a call back to "traditional" norms as justification for men's dominance over women. The imagery of purity, honor, and duty surrounding this rhetoric further intensifies the frequency and intensity of violence.

Regaining "Lost" Power

Online misogyny shifted the incel movement from a platform for discussion on the negative impacts of rigid gender norms to a forum for radicalization into violent action.[62] Central to the incel movement's rhetoric and beliefs is the idea that women are superficial beings who are only attracted to "genetically superior men" (referred to as "Chads").[63] The belief that women "stole" power from men has spurred physical attacks. Elliot Rodger, author of the 133-page "Manifesto on Women," conducted one such attack. Rodger shot eight people in Isla Vista, California, in 2014 before killing himself. Since Rodger's attack and the proliferation of his manifesto, there have been four copycat attacks: Chris Harper-Mercer (Umpqua Community College shooting in Los Angeles, California), William Atchison (Aztec High School in Aztec, New Mexico), Alek Minassian (van attack in Toronto, Canada), and Scott Beierle (hot yoga shooting in Tallahassee, Florida).[64] The rhetoric of these attackers shows the connection between the belief that power has been taken from them and the need to commit violence to right this injustice. As Alek Minassian posted on his Facebook page just before his attack:

> Private (Recruit) Minassian Infantry 00010, wishing to speak to Sgt 4chan please. C23249161. The Incel Rebellion has already begun! We will overthrow all the Chads and Stacys! All hail the Supreme Gentleman Elliot Rodger![65]

Incel forums promote the belief that women should be submissive to the natural power of men, and men should be able to exert their physical dominance and have sex without being rejected. Discussing familial relations, this is seen in patriarchal dominance:

> I'm more for Nathan Larson's version where the families are an individual entity and in that family the father decides where his daughter goes. I.E [*sic*] the father decides who the female marries to, and this can be at any age. The father, being the head of the household and the creator of the daughter, should also decide where she goes (as long as its [*sic*] monogamous, same race, heterosexual etc.).[66]

When society rejects them, they blame Western feminism for undermining the natural order.[67] Their rhetoric quickly turns to celebrating violence in this regard:

> Everytime i [*sic*] see on the news a woman that was raped, killed and whatnot. I just applaud the based one who took the time and effort to dispatch such useless garbage in the world.[68]

While their online rhetoric may sound abhorrent, the security threat comes from its translation into the physical world. In his own words during his interrogation with a police officer from the Toronto Sex Crimes Unit (identified in the transcripts as "THOMAS"), Alek Minassian explained how his participation on forums spurred him to action. The online environment was attractive because of the "style of conversation" of the members who shared his opinions and access to individuals like Elliot Rodger who he admired:

> MINASSIAN: I felt kind of proud of [Elliot Rodger] for his acts of bravery.
>
> THOMAS: Okay alright and what about how you started to . . . change your thinking? Was any of that going on [in your conversations]?
>
> MINASSIAN: I was starting to feel . . . radicalized at that time.
>
> THOMAS: When you say radicalized what do you mean by that?
>
> MINASSIAN: Meaning I felt it was time to take action and not just sit on the side lines and just . . . fester in my own sadness . . .
>
> THOMAS: Right but then as you got to know Elliot [Rodger] and understand his . . . mission and what he had done you began to become radicalized in terms of your thought process.[69]

Minassian goes on to discuss how his violent actions were celebrated in the online environment:

> MINASSIAN: Yes [after the attack] quite a few people . . . were congratulating me.
>
> THOMAS: Okay.
>
> MINASSIAN: And in fact I remember there was one poster who said he was from Edmonton and he would be planning a similar uprising in November . . . of this year.
>
> THOMAS: Of this year, okay, okay and what ah specifically did he say in terms of what he was going to do?
>
> MINASSIAN: He said . . . hey thanks man . . . you you've

> given me great inspiration, November 15 Edmonton the continuation of the rebellion.[70]

The amplification of misogynistic sentiments in the online environment has spurred direct violence. The case of the incel movement shows how the combination of the particularly violent form of masculinity practiced, coupled with the legitimacy granted by online forms has deadly consequences.

Return to Traditional Societies of Order, Honor, Duty, and Purity

ISIS frames itself fighting against the Western oppression of Muslim populations and aims to create its own political system across boundaries. More than 140 violent attacks have been claimed by ISIS, making it one of the deadliest terrorist organizations.

Most analysis of ISIS's propaganda and discourses focus on its rejection of the Western lifestyle. Most gendered analysis of ISIS focuses on the seemingly exceptional nature of their decision to deliberately recruit women.[71] Yet, a discourse analysis rooted in understanding the role of online misogyny shows a clear instrumentalization of gender norms as a catalyst for its violent action. In crafting recruitment messages, ISIS has created a narrow lane in which women are allowed to operate. Women can be mothers and wives and occasionally suicide bombers. ISIS uses this narrow view of a woman's role to deconstruct the narratives on gender equality promoted by the West:

> My Muslim sister, indeed you are a mujāhidah, and if the weapon of the men is the assault rifle and the explosive belt, then know that the weapon of the women is good behavior.[72]

The *Dabiq* column "To Our Sisters" directly addresses the perceived "harms" that Western feminism has enabled:

> Indeed, when the Sharī'ah of our Lord was eliminated, the laws and rulings of the kuffār gained power in the lands of the Muslims, Islam was shamefully abandoned, and faces turned towards promiscuous Europe, the voice of falsehood rose and with it the voices of those hostile towards the people of the religion, and the cancer of those who legislate besides Allah ate away at the Ummah's body. They prohibited what He permitted, and permitted what He prohibited, and one of the most manifest things that they ruined and defamed in defense of women and their rights—as they claimed—was polygyny. They utilized their podiums to that end, including the podiums of the kufrī parliaments and the secular TV channels, and placed on these podiums howling dogs, fools who do not per-

> ceive nor know their foolishness. Their poisoned words crept into the hearts of women from the lands of the Muslims, to the point that we almost couldn't find a single woman that is accepting of this issue, except for those whom Allah protected.[73]

In conjunction with promoting an ideal womanhood that stands counter to Western values, ISIS employs a gendered focus on humiliation to spur violence by Muslim men. They frame the occupation of territory as another example of how Western feminism is stripping power away from men. They amplify this through the use of imagery involving children and women to shame men. For example, in *Al-Rumiyah*:

> so what is the matter with those men who . . . continue to remain behind, having laid down their swords, even watching passively as they are surpassed on occasion by the women of the Ummah?! Such was the case on 11 September 2016, when three muwahhid [monotheist] sisters carried out a daring attack on a police station in Mombasa, Kenya, targeting the security forces of a Crusader nation, and doing so in support of the Islamic State. . . . With all three sisters attaining shahadah [martyrdom] after voluntarily shouldering a duty that Allah had placed on the shoulders of the men of the Ummah. . . . The Sunna of the Prophet directed its incitement for physical combat towards the men of the Ummah. Why, then, do so many men continue to neglect their duty? Why have they laid down their swords and armed themselves instead with one excuse after another for not fulfilling their obligation?. . . . And why have they sat back idly—if not cowardly—while the Ummah's chaste, noble women, for whom jihad is a voluntary and righteous deed, stood in all their bravery to fulfill the duty of men?!. . . . They can take a lesson from their courageous sisters. These men can learn what it means to be sincere to Allah by reading the last testament of their sisters in Kenya who have joined the ranks of the shuhada [martyrs].[74]

The online environment is used to broadcast recruiting messages. While their online magazine published in both English and Arabic allows ISIS to have an international audience, it also uses open platforms such as Telegram, Facebook, or YouTube to disseminate videos and imagery to shame men into joining their ranks. Such rhetoric plays on the discomfort men who hold traditional gendered beliefs experience at the thought of a woman or child being more empowered than them. It follows the pattern that Michael S. Kimmel finds in linking emasculating language to taking up arms against the West.[75] The persistence of attacks attributed to ISIS have continued even as political leaders in the United States and abroad have praised the "defeat" of ISIS's hold on territory. ISIS claimed responsibility for attacks that have resulted in more than 200 deaths in the first half of 2020 and continued its typical escalation in Syria during the holy month of Ramadan (24 April through 23 May) despite the COVID-19 pandemic.[76] The inspector general warns that attacks may continue to increase if pressure is reduced due to pandemic responses.[77] Indeed, the case of ISIS shows how the threat of violent extremism transcends physical territorial threats, and it illustrates the particularly dangerous role that the online environment plays in inciting violence.

Discussion

The Combined Security Threat

The cases of the U.S. military, the incel movement, and ISIS highlight the holistic nature of the security threat posed by online misogyny. The nature of attacks being perpetrated by violent radicalized groups such as the incel movement and ISIS have a very gendered dimension. To combat them, the military must take a gendered approach to understanding the security landscape. However, the very same phenomenon that is leading to these violent attacks is also hindering the military from recruiting and retaining the people needed to meet this threat.

The need for women in the military extends beyond meeting force strength numbers. The wars in Iraq and Afghanistan highlighted the operational necessity of women's service in culturally sensitive conflicts.[78] Women have unique, gendered roles that cannot be duplicated by their male counterparts.[79] Though the United States is pivoting away from its role in Iraq and Afghanistan, the gendered threat remains. As shown in the case of the incel movement, gendered extremism is not unique to the Middle East, and as the United States pivots to near-peer competition, understanding how cultural gendered norms contribute to violence will continue to be important. In the near-peer environment, cultural competency in the online environment will be a key factor in ensuring U.S. security. China and Russia are both adept at online disinformation campaigns. And while their disinformation is not necessarily misogynistic in nature, it is culturally specific. New research is highlighting the importance of diverse teams—especially gender diverse teams—at identifying online misinformation within specific cultural contexts.[80] An effective force of the future will require a broad recruitment pool.

Numerically, it should not be difficult to recruit women. In every state, women's Service eligibility outpaces men's by an average of 2 percent.[81] Women also have an increased high school graduation rate and are outpacing men in the science, technology, engineering, and math (STEM) fields, giving them the hard skills necessary to combat the growing online threat. This should be good news—as more women are needed, more are becoming eligible and have the desired skills for service. However, despite having a greater eligibility to serve, women have less than half of the propensity to serve as men—7 percent compared to 15 percent.[82] Further, women's propensity to serve has remained relatively unchanged—6 percent in 2001 compared to 7 percent in 2017—despite efforts by the Services to target their recruitment. Women feature prominently in the recruiting campaigns for all branches of the military. A prominent example of this is the Marine Corps' "Battles Won" recruitment campaign. The first ad in the campaign series, "Battle Up," features a female protagonist, tracing her life from high school student to Marine on the battlefield. This ad garnered a higher-than-average favorability rating (58 percent compared to 49 percent for all other ads) among all recruits, yet still did not lead to an increase in women's overall recruitment.[83] At the highest levels of government, this combined security threat has been recognized. The Department of Defense's (DOD) implementation guidance for the Women, Peace, and Security Act of 2017 directly addresses the need for a more diverse fighting force to counter today's threats.[84] Defense Objective 1 specifically addresses this, stating, "The Department of Defense exemplifies a diverse organization that allows for women's meaningful participation across the development, management, and employment of the Joint Force."[85] However, without addressing the threat of misogyny across the spectrum, this will not be met. There is evidence that the military is beginning to address online misogyny as a security threat. Threat briefings received at Joint Base Andrews, Maryland, in 2019 included a slide on incels in order to "educate commanders on the behaviors associated with the group to safeguard Airmen."[86] Secretary of Defense Lloyd J. Austin III is expanding these efforts. On 2 February 2021, he called for a Department of Defense-wide stand-down to address the risk of extremism among servicemembers.[87] Such efforts are an encouraging step, as the prevalence of harmful ideals is evidenced by participation by active duty military and veterans in the 6 January 2021 insurrection at the U.S. Capitol.[88]

In addition to hindering the United States' ability to meet force strength requirements, online misogyny continues to facilitate physical violence toward U.S. interests. The case of ISIS shows how territorial defeat alone is not enough to claim victory over an adversary. While U.S. security officials were focused on defeating the physical caliphate, ISIS continued to build support in the online environment, using hatred toward Western values of equality to recruit individuals and groups to commit violent attacks in areas beyond Iraq and Syria. A gendered approach will address many of these blind spots in security and result in greater overall security.

Recommendations

To combat the threats of online misogyny, the United States security sector—including the military—must fully internalize the importance of gendered approaches to security. To do this, it must not only recognize the importance of the online environment to national security but take a particular gendered approach to understanding how this domain impacts security. In the 20 years since the passage of United Nations Resolution 1325, there have been attempts at integrating women, peace, and security into security operations, yet both top-down and bottom-up attempts have fallen short of holistically addressing the threat that online misogyny poses.[89]

Recruiting more women into the security sector is clearly a start, but simply adding more women on its own is not enough. The security sector is a historically masculine enterprise and adheres to what Kyleanne Hunter and Rebecca Best describe as cognitive-institutional reinforcement.[90] The military and other aspects of the security sector are institutions that rely heavily on a masculine view of warfighting and have historically expected women to adhere to these norms when they join. This requires women to act like "little men" to be successful. This not only has an impact on women's identities but undermines the ability of the military to leverage women's perspectives. When integrating women, the military must do so in such a way that allows them to maintain their unique perspectives.

This requires addressing training, education, and equipment. Fully integrating all training units is a necessary first step. Gender-integrated teams perform better at solving complex problems and do so more successfully when they build task-based cohesion during initial training. Separating men and women during training reinforces the idea that women's perspectives are inferior to men's, while integration builds better teams and sets a baseline for acceptance and appreciation of the unique perspectives women bring.[91] Beyond initial training, gender perspectives must be integrated into all levels of military education to reaffirm and recognize the importance of women's perspectives. While top-level civilian leaders have recognized the importance of women's perspectives, operational commanders have dismissed women's perspectives as secondary to traditional hard security outcomes.[92] Introducing the connection between women's security and hard security outcomes throughout military education will result in more robust security outcomes.

The nature of military equipment also has an important role in ensuring that women's unique perspectives are appreciated and integrated. Ill-fitting equipment not only results in an increased likelihood that women servicemembers will be injured but also creates a cultural feeling that women ought to be little men.[93] Properly fitting equipment, conversely, optimizes women's performance and allows for them to not only better contribute to military missions but to do so while building a culture that also respects them and leverages their unique skills.[94] Indeed, through training and equipping, the military Services can meaningfully address some of the underpinnings of misogyny and leverage the unique skills of women to combat broader security threats. While the military has made strides in integrating gendered perspectives into some aspects of warfare, information and cyber warfare are lacking in this regard.[95] Yet as shown here, gendered activity, specifically online misogyny, is responsible for increased violence.

Taking a gendered approach to online activity and propaganda will also help with countering violent extremism efforts (CVE). CVE focuses on using noncoercive measures to dissuade radicalization.[96] A more nuanced understanding of gender and how misogyny is manifested is necessary to effectively understand the drivers of online misogyny and how to dissuade individuals from becoming radicalized online. A DOD-sponsored review that takes a gendered perspective to online radicalization both at home as well as in key potential hotbeds is a necessary first step. Such an approach should be three-pronged. First, it should include current and post-conflict countries (such as Iraq, Syria, and Afghanistan) from which groups like ISIS typically recruit. Second, it must include new hotbeds of recruitment—primarily the United States' European allies—as well as an internal review. The current global pandemic has exposed new economic and social tensions that may increase the likelihood of radicalization. And third, it must include our near-peer competitors in Russia and China to uncover how they are using gender to further disinformation.

Government counterterrorism and intelligence services must also recognize gender-driven violence as a form of extremism. This will have a two-pronged impact. First, it will empower local law enforcement to take meaningful action against extremism. And second, it will help to legitimize and guide private actors working in the combating violent extremism sector. Activities in Canada offer an example. In 2019, the Canadian Security Intelligence Service recognized gender-driven violence as a form of ideologically motivated violent extremism. That year, police charged a 17-year-old who had murdered a young woman with a machete in a massage parlor with "incel ideology," a first of its kind charge.

The Global Internet Forum to Counter Terrorism and Tech Against Terrorism have developed the Terrorist Content Analytics Platform (TCAP). TCAP alerts users to content associated with designated terrorist organizations, archives the material, and facilitates discussion between online platforms, civil society, law enforcement, and academia to improve classification and moderation of illegal content. Their classification depends on official designations of terrorist entities. The Canadian Security Intelligence Service recognition of gender-driven violence as a form of ideologically motivated violent extremism, and the recent addition of The Base and The Proud Boys to the list of terrorist organizations is allowing for online misogyny to be captured. While it is too soon to know the impact of these changes, this is promising for ensuring early warnings of violence.

The Violence Against Women Act (VAWA) is an additional policy that has promise for combating this form of online extremisms. President Joseph R. Biden made passing the reauthorization of VAWA a centerpiece of his campaign. As his administration pushes for the policy, it has the opportunity to include legislation against online gendered abuse. Despite the legal complexity of attribution in online violence, lawmakers have an opportunity to strengthen legal protections and implement early detection of potential violence.

This comprehensive gendered approach will address both the internal and external security threats posed by online misogyny. It will also reduce the prevalence of the form of misogyny most associated with violence. Empirical evidence shows that ensuring gender equality at the structural level reduces the likelihood of the forms of violence most associated with hegemonic masculinity—including rape (or the threat thereof), intimate partner violence, and politically motivated attacks against women.[97]

It also will help to reduce the firehose of falsehood. More comprehensive gendered approaches to security in the online environment will ensure that fewer pieces of disinformation fall through the cracks. As men and women are socialized differently, they are able to identify different aspects of disinformation.[98] Deliberately ensuring that diverse perspectives are part of the totality of security operations will help to detect early signs of misogynistic disinformation and ultimately keep the United States more secure.

Conclusion and Future Research

Online misogyny is a form of information warfare that the United States military must take more seriously. As demonstrated in this article, there are both external and internal risks posed by the unchecked presence of online misogyny. Security sector reform that adopts a holistic gendered perspective is one way to address this threat. There are two additional potential solutions that the authors' work can help inform: the role of private companies and the viability of an ecological approach to fighting online misogyny.

The focus of this article has been to identify the existence and severity of the security threat posed by online misogyny. Yet, cybersecurity is the responsibility of organizations beyond the military. Most social media platforms are privately owned and have a broad transnational presence. This raises questions about the responsibility of the organizations that administer online platforms to monitor activities that occur on them and who is able to enforce rules and regulations that may apply to them. Section 230 of the Communications Decency Act of 1996 has shielded technology companies from lawsuits and responsibility for content published on their platforms. However, Twitter's decision to permanently suspend former President Trump's account has opened new discussions on how tech companies should proactively engage with potentially dangerous speech. A report from the U.S. Department of Justice argues that Section 230 should be revised to "reflect the realities of the modern digital age," including online gendered abuse, doxing, and encouraging political violence.[99] This article emphasizes the need to ensure that both implicit and explicit bias in tech is studied in more meaningful ways. As we have shown, online misogyny has been historically overlooked as a security threat. There is need for more research into how this historic omission has shaped bias in automated threat identification and what aspects may have fallen through the cracks.

While the online environment has created the platform used to springboard online misogyny into physical security threats, technology solutions alone will not solve the problem. An ecological approach addresses all potential factors—social, economic, environmental, health (both physical and mental), and structural—that contribute to the security threat posed by online misogyny. Rather than addressing the consequences of online misogyny, a prevention strategy based on addressing needed social, medical, or educational services aims to address root causes.[100] However, additional research is needed to determine what factors are necessary to inform an ecological approach to specifically address online misogyny. Many actions and beliefs that could potentially be included in the misogynistic panoply are deeply embedded into our public institutions.[101] Interdisciplinary work in psychology, sociology, security studies, and public health is needed to determine the factors most frequently associated with individuals susceptible to engaging in the types of misogyny that result in security threats and create meaningful diversion programs. Online misogyny should not be dismissed as an overreaction on the part of feminists or diminished to simply disliking women. It presents a real security threat that has multifaceted consequences. It is neither merely boys behaving poorly on the internet, nor are its impacts only on women. Taking a gendered approach to security is a necessary first step in addressing some of the most harmful aspects of online misogyny, but there remains significant work to be done as well. As a new topic, combating this form of information warfare will benefit from research in the technological sectors, as well as multidisciplinary research to address the drivers of misogyny.

Endnotes

1. Stuart A. Thompson and Charlie Warzel, "They Used to Post Selfies. Now They Are Trying to Overthrow the Election," *New York Times*, 14 January 2021.
2. Cynthia Enloe, *Bananas, Beaches and Bases: Making Feminist Sense of International Politics*, 2d ed. (Berkeley: University of California Press, 2014), 1.
3. Alice Marwick and Rebecca Lewis, *Media Manipulation and Disinformation Online* (New York: Data & Society Research Institute, 2017).
4. Debbie Ging and Eugenia Siapera, "Special Issue on Online Misogyny," *Feminist Media Studies* 18, no. 4 (2018): 515–24, https://doi.org/10.1080/14680777.2018.1447345.
5. Danielle Keats Citron, "Cyber Civil Rights," *Boston University Law Review* 89, no. 61 (2009): 61.
6. Enloe, *Bananas, Bases and Beaches*.
7. Bradley C. Nindl et al., "Operational Physical Performance and Fitness in Military Women: Physiological, Musculoskeletal Injury, and Optimized Physical Training Considerations for Successfully Integrating Women into Combat-centric Military Occupations," *Military Medicine*, no. 181 (2016): 50–62, https://doi.org/10.7205/MILMED-D-15-00382; and Corey Yung, "How to Lie with Rape Statistics: America's Hidden Rape Crisis," *Iowa Law Review* 99, no. 1197 (2014): 1197–1256.
8. Synne Laastad Dyvik, "Women as 'Practitioners' and 'Targets': Gender and Counterinsurgency in Afghanistan," *International Feminist Journal of Politics* 16, no. 3 (2014): 410–29, https://doi.org/10.1080/14616742.2013.779139.
9. Valerie M. Hudson et al., *Sex and World Peace* (New York: Columbia University Press, 2012).
10. The *manosphere* is the term given to those online spaces where anti-feminist propaganda is spread. For a discussion on the manosphere, see Debbie Ging, "Alphas, Betas, and Incels: Theorizing the Masculinities of the Manosphere," *Men and Masculinities* 22, no. 4 (2019): 63857, https://doi.org/10.1177/1097184X17706401.
11. Christopher Whyte, "Protectors without Prerogative: The Challenge of Military Defense against Information Warfare," *Journal of Advanced Military Studies* 11, no. 1 (Spring 2020), https://doi.org/10.21140/mcuj.2020110108; and Mariarosaria Taddeo, "Information Warfare: A Philosophical Perspective," *Philosophy & Technology* 25 (2011): 105–20, https://doi.org/10.1007/s13347-011-0040-9.
12. A most different research design is a quasi-experimental design that compares cases that are maximally different on all but the variable of interest. For a detailed discussion on the practice and applicability of most different designs, see Carsten Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research," *International Journal of Social Research Methodology* 11, no. 5 (2008): 389–401, https://doi.org/10.1080/13645570701401552. The term *incel* refers to a member of an online community of young men who consider themselves unable to attract women sexually, and they are typically associated with views that are hostile toward women and men who are sexually active.
13. Kate Manne, *Down Girl: The Logic of Misogyny* (New York: Oxford University Press, 2017).
14. Michael A. Messner, *Politics of Masculinities: Men in Movements* (Thousand Oaks, CA: Sage Publications, 1997), 9.
15. Ging, "Alphas, Betas, and Incels."
16. Peter Glick and Susan T. Fiske, "An Ambivalent Alliance: Hostile and Benevolent Sexism as Complementary Justifications for Gender Inequality," *American Psychologist* 56, no. 2 (February 2001): 109, https://doi.org/10.1017/CBO9781139022736.005; Małgorzata Mikołajczak and Janina Pietrzak, "Ambivalent Sexism and Religion: Connected through Values," *Sex Roles* 70, nos. 9–10 (2014): 387–99, https://doi.org/10.1007/s11199-014-0379-3; and Miguel Moya et al., "It's for Your Own Good: Benevolent Sexism and Women's Reactions to Protectively Justified Restrictions,"

Personality and Social Psychology Bulletin 33, no. 10 (2007): 1421–34, https://doi.org/10.1177/0146167207304790.

17. Cliff Cheng, "Marginalized Masculinities and Hegemonic Masculinity: An Introduction," *Journal of Men's Studies* 7, no. 3 (1999): 295–315, https://doi.org/10.3149/jms.0703.295; James W. Messerschmidt, *Hegemonic Masculinity: Formulation, Reformulation, and Amplification* (Lanham, MD: Rowman & Littlefield, 2018); and Yvonne Hirdman, "State Policy and Gender Contracts: The Swedish Experience," in *Women, Work and the Family in Europe*, ed. Eileen Drew, Ruth Emerek, and Evelyn Mahon (London: Routledge, 1998).
18. Susan Moller Okin, "Gender Inequality and Cultural Differences," *Political Theory* 22, no. 1 (1994): 5–24, https://doi.org/10.1177/0090591794022001002.
19. Ruth Roach Pierson, "Beautiful Soul or Just Warrior: Gender and War," *Gender & History* 1, no. 1 (March 1989): 77–86, https://doi.org/10.1111/j.1468-0424.1989.tb00237.x.
20. M. Christina Santana et al., "Masculine Gender Roles Associated with Increased Sexual Risk and Intimate Partner Violence Perpetration among Young Adult Men," *Journal of Urban Health* 83, no. 4 (July 2006): 575–85, https://doi.org/10.1007/s11524-006-9061-6.
21. Pablo Castillo Díaz and Nahla Valji, "Symbiosis of Misogyny and Violent Extremism: New Understandings and Policy Implications," *Journal of International Affairs* 72, no. 2 (2019): 37–56.
22. Elin Bjarnegård, Karen Brounéus, and Erik Melander, "Honor and Political Violence: Micro-Level Findings from a Survey in Thailand," *Journal of Peace Research* 54, no. 6 (November 2017): 748–61, https://doi.org/10.1177/0022343317711241.
23. Joshua M. Roose, *The New Demagogues: Religion, Masculinity and the Populist Epoch* (Abingdon, UK: Routledge, 2020).
24. Joseph A. Vandello et al., "Precarious Manhood," *Journal of Personality and Social Psychology* 95, no. 6 (December 2008): 1325–39, https://doi.org/10.1037/a0012453.
25. Chrystie Myketiak, "Fragile Masculinity: Social Inequalities in the Narrative Frame and Discursive Construction of a Mass Shooter's Autobiography/Manifesto," *Journal of the Academy of Social Sciences*11, no. 4 (2016): 289–303, https://doi.org/10.1080/21582041.2016.1213414.
26. Myketiak, "Fragile Masculinity."
27. Laura Bates, *Men Who Hate Women: From Incels to Pickup Artists: The Truth about Extreme Misogyny and How It Affects Us All* (New York: Simon and Schuster, 2020).
28. Ging, "Alphas, Betas, and Incels."
29. Whyte, "Protectors without Prerogative."
30. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: Rand, 2016), https://doi.org/10.7249/PE198.
31. Oksana N. Berduygina, Tatyana N. Vladimirova, and Elena V. Chernyaeva, "Trends in the Spread of Fake News in Mass Media," *Media Watch* 10, no. 1 (2019): 122–32, https://doi.org/10.15655/mw/2019/v10i1/49561.
32. Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (2018): 1146–51, https://doi.org/10.1126/science.aap9559.
33. The Pareto Principle, named after the economist Vilfredo Pareto, claims that 80 percent of consequences come from 20 percent of the causes, asserting an unequal relationship between inputs and outputs. However, this principle does not apply to sexual intercourse. CDC data show that 98 percent of women and 97 percent of men between the ages of 25–44 have had heterosexual intercourse. Anjani Chandra et al., "Sexual Behavior, Sexual Attraction, and Sexual Identity in the United States," *National Health Statistics Report* 3, no. 36 (March 2011): 36; and Gregory Newbold, "What Tempers the Steel of a Marine Corps Infantry Unit," *War on the Rocks*, September 2015.
34. John Corner, "Fake News, Post-Truth and Media–Political Change," *Media, Culture*

and Society 39, no. 7 (2017): 1100–7, https://doi.org/10.1177/0163443717726743.

35. The CDC's report, based on more than 18,000 telephone survey responses in the United States, estimates that roughly 5,365,000 men had been victims of intimate partner physical violence in the previous 12 months, compared with 4,741,000 women. However, the general assessment is that more than 1 in 3 women (35.6 percent) and more than 1 in 4 men (28.5 percent) in the United States have experienced rape, physical violence, and/or stalking by an intimate partner in their lifetime. The numerical difference is due to the survey sample size and is not indicative of a higher instance rate of sexual violence for men than women. For reference of how it is depicted on Incels.co, see "Scientific Blackpill," Incels.wiki, accessed 7 April 2021.

36. Ebuka Elias Igwebuike and Lily Chimuanya, "Legitimating Falsehood in Social Media: A Discourse Analysis of Political Fake News," *Discourse & Communication* 15, no. 1 (2021): https://doi.org/10.1177/1750481320961659; and Maria Giovanna Sessa, "Misogyny and Misinformation: An Analysis of Gendered Disinformation During the COVID-19 Pandemic," disinfo.eu, 4 December 2020.

37. Carsten Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research," *International Journal of Social Research Methodology* 11, no. 5 (2008): 389–401, https://doi.org/10.1080/13645570701401552.

38. Simona Frenda et al., "Online Hate Speech against Women: Automatic Identification of Misogyny and Sexism on Twitter," *Journal of Intelligent & Fuzzy Systems* 36, no. 5 (2019): 4743–52, https://doi.org/10.3233/JIFS-17 9023.

39. Office of People Analytics, "Updates on Female Recruiting Market" (PowerPoint presentation, Defense Advisory Committee on Women in the Services, September 2018); and Kyleanne Hunter, "We Need What Women Bring to the Fight," *War on the Rocks*, 21 September 2015.

40. Marianne W. Jørgensen and Louise J. Phillips, *Discourse Analysis as Theory and Method* (London: Sage Publications, 2002).

41. The full video of his interrogation was ordered to be made public by Justice Anne Molloy of the Ontario Superior Court on 27 September 2019. Nicole Brockbank, "Alek Minassian Reveals Details of Toronto Van Attack in Video of Police Interview," CBC, 27 September 2019.

42. Jennifer Hickes Lundquist, "Ethnic and Gender Satisfaction in the Military: The Effect of a Meritocratic Institution," *American Sociological Review* 73, no. 3 (2008): 477–96, https://doi.org/10.1177/000312240807300306; and Megan MacKenzie, *Beyond the Band of Brothers: The US Military and the Myth That Women Can't Fight* (Cambridge, UK: Cambridge University Press, 2015), https://doi.org/10.1017/CBO9781107279155.

43. *An Overview of Social Media Trends* (Alexandria, VA: Office of People Analytics, 2020), 7.

44. Maggie Fox and Erika Edwards, "Teens Spend an 'Astounding' Nine Hours a Day in Front of Screens: Researchers," West Virginia Education Institution, accessed 12 March 2021.

45. Focus group, Defense Advisory Committee in the Services, 2015–19. For all focus groups, all identifying information—to include bases and locations—have been removed to protect anonymity.

46. Focus group, Defense Advisory Committee in the Services, 2015–19.

47. There is evidence from nonmilitary contexts showing the relationship between women's sociopolitical advancement and a resulting violent backlash. The Women's Rights After War Project led by Marie E. Berry and Milli Lake is the most extensive examination of this phenomenon. Based on research in 10 countries, it found that as women obtained political and social power, they were more likely to experience violence and social backlash by men. See Sinduja Raja, Marie E. Berry, and Milli Lake, "Women's Rights After War," *FBA Research Brief* (December 2020). Berry and Lake's findings echo research in the corporate sector. This research dates back to the 1990s, where the business world was looking to understand ways in which to accelerate women's growth

in corporate America, but found that backlash at the hands of fellow employees was the most common result of success. See, for example, Ronald J. Burke and Susan Black, "Save the Males: Backlash in Organizations," *Women in Corporate Management* 16, no. 9 (June 1997): 61–70, https://doi.org/10.1007/978-94-011-5610-3_7.

48. Kyleanne Hunter and Jeannette Haynie, "The Marines United Scandal Should Be Seen as a National Security Threat," *Foreign Policy*, 13 April 2017.
49. *All Marines Message 008/17, Social Media Guidance—Unofficial Internet Posts* (Washington, DC: Headquarters Marine Corps, 2017).
50. Focus group, Defense Advisory Committee in the Services, 2015–19.
51. Focus group, Defense Advisory Committee in the Services, 2015–19.
52. Dave Phillips and Tim Arango, "Who Signs Up to Fight? Makeup of U.S. Recruits Shows Glaring Disparity," *New York Times*, 10 January 2020.
53. *An Overview of Social Media Trends*.
54. Army Enterprise Marketing Office, "Current Army Marketing Strategy" (PowerPoint presentation, Office of the Assistant Secretary of the Army [Manpower and Reserve Affairs] to the Defense Advisory Committee on Women in the Services, Arlington, VA, 5 December 2019).
55. Focus group, Defense Advisory Committee in the Services, 2015–19.
56. Focus group, Defense Advisory Committee in the Services, 2015–19.
57. Focus group, Defense Advisory Committee in the Services, 2015–19.
58. Focus group, Defense Advisory Committee in the Services, 2015–19.
59. Focus group, Defense Advisory Committee in the Services, 2015–19.
60. *Female Active-Duty Personnel: Guidance and Plans Needed for Recruitment and Retention Efforts* (Washington, DC: Government Accountability Office, 2020).
61. Leo Braudy, *From Chivalry to Terrorism: War and the Changing Nature of Masculinity* (New York: Alfred A. Knopf, 2003).
62. The first incel forum was created in 1997 by Alana, a bisexual woman. The Alana's Involuntary Celibacy Project (AICP) was supposed to be a platform where people could connect and discuss their loneliness. However, men and latent sexism took over the forum and transformed it into self-hatred, scapegoating, and violence.
63. Ging, "Alphas, Betas, and Incels."
64. The decentralized nature of the incel movement and the historic omission of misogyny being recognized as a hate crime makes knowing the exact number of incel-inspired attacks difficult. Based on our research, the following other prominent attacks likely fall into this category: Marc Lepine, the perpetrator of the school shooting at the École Polytechnique de Montréal on 6 December 1989; George Sodini, who shot 12 women in an aerobics class in Pittsburgh, PA, on 4 August 2009; Sheldon Russell Bentley, who killed a man in a mall supermarket in Edmonton, Alberta, on 21 July 2016; Nikolas Cruz, who killed 17 people at Marjory Stoneman Douglas High School in Parkland, FL, on 14 February 2018; and a 17-year-old (name withheld since he is a minor) who stabbed three people at a Toronto massage parlor on 24 February 2020.
65. Facebook post recovered from https://www.thestar.com/news/gta/2018/04/25/number-cited-in-cryptic-facebook-post-matches-alek-minassians-military-id-source.html.
66. Retrieved from the incels.co forum.
67. *When Women Are the Enemy: The Intersection of Misogyny and White Supremacy* (New York: Anti-Defamation League, 2018).
68. Retrieved from the incels.co forum at https://incels.co/threads/why-you-should-never-feel-any-remorse-for-women.259615/.
69. "Electronically Recorded Interview of Alek Minassian by Detective Robert Thomas (3917) of the Sex Crimes Unit Polygraph Unit on Monday, April 23, 2018, at 2246 Hours."
70. "Electronically Recorded Interview of Alek Minassian by Detective Robert Thomas (3917) of the Sex Crimes Unit Polygraph Unit on Monday, April 23, 2018, at 2246 Hours."
71. Alice Martini, "Making Women Terrorists into 'Jihadi Brides': An Analysis of Media Narratives on Women Joining ISIS," *Critical Studies on Terrorism* 11, no. 3 (2018):

458–77, https://doi.org/10.1080/17539153.2018.1448204; Elizabeth Pearson, "The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad," *Policy and Internet* 8, no. 1 (March 2016): 5–33, https://doi.org/10.1002/poi3.101; *Testimony before the House Foreign Affairs Committee*, 114th Cong. (28 July 2015) (testimony of Kathleen Kuehnast, "How ISIS Exploits Children by Manipulating Gender Dynamics"); and Leah Windsor, "The Language of Radicalization: Female Internet Recruitment to Participation in ISIS Activities," *Terrorism and Political Violence* 32, no. 3 (January 2018): 1–33, https://doi.org/10.1080/09546553.2017.1385457.

72. *Dabiq Magazine*, no. 11, 44.
73. *Dabiq Magazine*, no. 12, 19.
74. Haroro J. Ingram, "Rallying the 'True Believers' as Hardship Purifies the Ranks," *Al-Rumiyah*, no. 2 (October 2016).
75. Michael Kimmel, *Healing from Hate How Young Men Get Into—and Out of—Violent Extremism* (Oakland: University of California Press, 2019).
76. *Operation Inherent Resolve: Lead Inspector General Report to the United States Congress* (Washington, DC: Department of Defense, 2020), 18.
77. *Operation Inherent Resolve*, 19.
78. Kyleanne Hunter, "In Iraq We Were Never Neutral," *Journal of Veteran Studies* (forthcoming 2021).
79. Maj Ginger E. Beals, "Women Marines in Counterinsurgency Operations: Lioness and Female Engagement Teams" (master's thesis, Marine Corps Command and Staff College, 2010).
80. Nicole A. Cooke, *Fake News and Alternative Facts: Information Literacy in a Post-Truth Era* (Chicago, IL: American Library Association, 2018).
81. Office of People Analytics, "Updates on Female Recruiting Market."
82. Office of People Analytics, "Updates on Female Recruiting Market."
83. "DACOWITS Quarterly Business Meeting" (PowerPoint presentation, Arlington, VA, 5 December 2019).
84. *Women, Peace, and Security: Strategic Framework and Implementation Plan* (Washington, DC: Department of Defense, 2020).
85. *Women, Peace, and Security*, 12.
86. Jared Keller, "This Is a Real Slide from an Air Force Brief on the Real Threat of Incels," *Task & Purpose*, 20 June 2019.
87. Jim Garamone, "Austin Orders Military Stand Down to Address Challenges of Extremism in the Ranks," Department of Defense, 3 February 2021.
88. An analysis by NPR found that 20 percent of those charged in the aftermath of the insurrection were serving or had served in the military.
89. "Landmark Resolution on Women, Peace and Security," OSAGI, accessed 24 March 2021. UN Security Council Resolution 1325, passed October 2000, was the first formal Security Council resolution to recognize the role that women play in international peace and security, and to call for an increase of women in the security sector.
90. Kyleanne Hunter and Rebecca Best, "You Can't Have Women in Peace without Women in Conflict and Security," *Georgetown Security Studies Review* 8, no. 2 (November 2020): 5–18.
91. Emerald M. Archer, "The Power of Gendered Stereotypes in the US Marine Corps," *Armed Forces & Society* 39, no. 2 (2013): 359–91, https://doi.org/10.1177/0095327X12446924; and Kyleanne Hunter, "Of Methodology and Men," Political Violence at a Glance, 6 October 2015.
92. Kyleanne Hunter, Jeannette Haynie, and Natalie Trogus, "A Cornerstone of Peace: Women in Afghanistan," Warroom, 8 January 2021.
93. Kate McGraw, "Gender Differences among Military Combatants: Does Social Support, Ostracism, and Pain Perception Influence Psychological Health?," *Military Medicine*, no. 181 (2016): 80–85, https://doi.org/10.7205/MILMED-D-15-00254.
94. Nindl et al., "Operational Physical Performance and Fitness in Military Women," 50–62.

95. Most notably, the importance of women is highlighted in both the Army and Marine Corps counterinsurgency manuals (*Counterinsurgency*, Field Manual 3-24, and *Insurgencies and Countering Insurgencies*, Marine Corps Warfighting Publication 3-33.5, respectively). Mahlet Abera Techan, "Gendering Cyber Warfare: A Theoretical and Exploratory Paper Addressing the Research Gap on the Gendered Aspects of Cyber Warfare" (PhD diss., Upsalla University, 2020).

96. Humera Khan, "Why Countering Extremism Fails: Washington's Top-Down Approach to Prevention Is Flawed," *Foreign Affairs*, 18 February 2015.

97. Hudson, *Sex and World Peace*.

98. Cooke, *Fake News and Alternative Facts*.

99. *Section 230—Nurturing Innovation or Fostering Unaccountability?* (Washington, DC: Department of Justice, 2020). The term *doxing* refers to publicly revealing private personal information about a person or company.

100. An example of a successful program on which these interventions are based can be found at Stevan M. Weine and Heidi Ellis, "Mobilizing Mental Health Resources Offers Hope to Countering Violent Extremism," MDedge, 25 February 2015.

101. Hunter and Best, "You Can't Have Women in Peace without Women in Conflict and Security."

Consistency of Civil-Military Relations in the Israel Defense Forces
The Defensive Mode in Cyber

Glen Segell, PhD

Abstract: The Israel Defense Forces (IDF) has four battle threats, where cyber is equitable to conventional (state), subconventional (nonstate), and nonconventional. An escalation in one could lead to an overall escalation in all. In the political areas and, by extension, in civil-military relations (CMR), the IDF has a defensive mode as routine, while an offensive mode is manifest rarely in emergencies and war. The IDF is engaged in a total war in a defensive mode yet a limited war in the offensive mode as Israel's adversaries do not share the same policies with regular cyber and terror attacks against civilian, government, and military targets. There is consistency in all four threats. Fencing, active defense, and preventive and preemptive strikes dominate.

Keywords: Israel Defense Forces, IDF, civil-military relations, CMR, cyber, limited war, total war, deterrence, defensive mode

Introduction

In 2014, the then-chief of the General Staff of the Israel Defense Forces (IDF *tsahal* צה"ל), Lieutenant General Gadi Eizenkot, created the first cyber branch within the IDF to consolidate all of Israel's cyber capabilities into a single entity.[1] In 2015, Eizenkot authorized the first-ever release of the *Israel Defense Forces Strategy Document* (hereafter *IDF Strategy Document*) to the pub-

Dr. Glen Segell is a research fellow at the Ezri Center for Iran and Gulf States Research, University of Haifa, Israel, and in the Department of Political Studies and Governance, University of the Free State, South Africa. He specializes in intelligence studies, civil-military relations, and strategic communications. He holds the rank of brigadier general (Reserves), where he also consults as an expert for the North Atlantic Treaty Organization (NATO). He was in active intelligence and offense operations in Iraq, Kuwait, Sudan, and Libya.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201004

lic realm. It informed the public of the IDFs' efforts in planning, preparation, training, and defense to meet all threats including cyber, where an escalation in one battle space could also be, or lead to, an escalation in others, especially if the adversaries were the same.[2] The IDF spokesperson stated that the purpose of the document was to "provide a systemic analysis and definition of the context in which the concept was developed."[3] In 2018, Eizenkot for the first time located cyber as the fourth realm of battle threats and spaces alongside other weapons and spaces of operation, namely land, sea, and air. The three other battle threats are conventional (state), subconventional (nonstate), and nonconventional.[4]

This article examines the consistency of civil-military relations (CMR) for all four battle threats and spaces. Such consistency is evident in a combined and joint conformity in the decision making of the civilian government and the application or implementation of these decisions by the military. A policy decision by the civilian government and the military implementation of the decision on the tactical level action for one battle threat and space is the same for the others. This shows that the conformity is in the act of matching attitudes, beliefs, and behaviors to norms, politics and like-mindedness. The norms are implicit, specific rules shared by the civilian government and the military on who is the adversary and how to defeat them that guide their interactions with each other in civil-military relations. This consistency of behaving or performing in the same manner is for all four battle threats and spaces.

The consistency is evident, for example, if an attack and an attacker are a combination of intent and means in any space, then there is no reason why cyber should be treated any differently in the decision making of civil-military relations to that of an attack in the subconventional (nonstate) space, especially if it is the same attacker, for example Hamas. For Israel, it is the same attackers/adversaries in all four spaces and for all four battle threats; in 2021, these include Iran and Iranian proxies such as Hezbollah and Hamas as well as other smaller but more extremist Islamic groups such as the Islamic Jihad Movement in Palestine. In CMR, it is the same democratically elected civilian leaders that have the parliamentary (Israel Knesset) legitimacy and authority to determine the political direction for the IDF to engage in combat against them. Following the process and procedures of CMR, it is the IDF and its soldiers that are tasked with implementing the political decisions. The generals and the soldiers are the professionals who can decide on the best means to do so, commonly known as strategy and tactics.

Commentators in Israeli think tanks speculated that when Eizenkot made the document public for the first time in 2015, it was the fourth of this type of document written since 2002. The goal of the documents had CMR in mind to increase the transparency between the IDF, the political echelon, and the public as a response to the absence of official national security documents.[5] Transparency and openness was indeed a unique act, yet the content was not a surprise. The content served only to confirm in writing what was already known about the consistency in CMR; in CMR, and by extension in Israeli strategy, both the democratically elected civilian government and the military have a central core of generally shared organizing ideas concerning its national security. That is that the broad purpose of Israel's strategy is the deterrence of aggression and the clear-cut defeat of the enemy if deterrence fails.[6]

In Israeli CMR, there is no evidence that the civilian government seeks military versus political solutions. Rather, it is standard for them to consult with the defense and security organizations to calculate the consequences and ramifications of any decision when engaging adversaries, including considering casualties, and in doing so the most frequent decision is to prefer defense and diplomacy over war. By extension in CMR, the IDF is subservient to the elected civilian leadership of when to go to combat and against whom but decides how to implement the war. The security concept of this has three basic pillars: deterrence, early warning, and decisive defeat (*hachra'a הכריע*) as the basis for the thinking of being in a strategically defensive mode as routine for all four battle threats and spaces.

Routine is a sequence of actions regularly followed. It is the regular procedure. It is the most accurate translation possible of the Hebrew word (*shigra* שגרה) used in the IDF regularly to indicate no changes for daily military activities in any unit. Such a routine is differentiated from an action or procedure that is undertaken or performed for a special reason. While the defensive mode is routine on a daily basis, an offensive mode is manifest only rarely for a special reason such as in emergencies and in escalations to counterinsurgency battles and war.[7]

With the progression of technology, active defense has been added to this routine military toolbox of defense and deterrence. Active defense serves to support the offense when required, and this in effect enables IDF thinking to be operationally offensive as part of the defensive, or in other words to act in preventive or preemptive combat. One area where active defense thinking prevails is when answering, "What is to be defended?" or when discerning between defense and protection. Defense may be repulsing enemy forces attempting to enter territory, while protection is evident, for example in fencing, in antimissile/rocket systems such as the Iron Dome system, and in cyber.[8]

In operationally offensive cyber, using active defense could be manifest as "defensive cyberspace operations—response action" (DCO-RA). These are those "deliberate, authorized defensive actions which are taken to defeat ongoing or imminent threats."[9] Here then is a case of the consistency in CMR for the four battle threats and spaces. It is also where the security concept in practice links kinetic (conventional) with cyber in combat. This was evident, for example, in 2007 when the IDF employed cyber capabilities and electronic attacks to suppress an enemy air defense network so that Israeli Air Force jets could destroy a suspected nuclear facility in Syria.[10]

The defensive mode is evident also in daily routine as few of the male and female conscripts in the IDF see combat during their national service. The majority of the 10 percent of conscripts who are in frontline combat are in the land forces where a majority spend most of their service in training and on border patrols. The rest are in support roles. Similarly, those in the navy spend most of their time in training and patrols with few interdictions or skirmishes.[11] Yet for those in air there is more combat; for example, in 2020, there were more than 500 bombings of munitions and convoy targets in Syria. Those serving in cyber units, although not in physical combat, are more likely to defend against cyberattacks, though they might also be engaged regularly in DCO-RA support.[12]

This article will continue to set the case to test the hypothesis of the consistency in CMR for all four battle spaces and threats, with the IDF engaged in a total war in a defensive mode as routine, yet a limited war in the offensive mode in emergencies, escalations to counterinsurgency, and war. This will be examined in three sections, each with subsections. The first section provides definitions and outlines the concepts examined, including lessons for cyber from conventional and subconventional battle threats, limited and total wars, and limited cyber battles. The second section provides examples that examine the hypothesis, including planning and preparation, authority and jurisdiction, fencing the battle terrain, and mapping the battle terrain. The third section examines how cyber evolved to the significance of being a battle threat and space equitable to the others based on three time frames: the first period from 1993–2003, the second period from 2004–13, and the final period from 2014 to the present.

The Consistency of the Defensive Mode across the Four Battle Threats

This section provides definitions and outlines the concepts of Israel's defense doctrine that views war as the "no choice option," which carries a heavy social and economic price tag. Therefore, Israeli doctrine relies heavily on the defensive mode that includes the projection of deterrence.[13] There are three subsections: lessons for cyber from conventional and subconventional battle threats, limited and total wars, and limited cyber battles.

Lessons for Cyber from Conventional and Subconventional Battle Threats

The military duration of Israel's three interstate conventional wars before the cyber age were the Suez Crises (1956) for one week and two days, the Six Day War (1967) for six days, and the Yom Kippur War (1973) for two weeks and five days. Such decisive conventional victories may well have deterred more interstate conventional wars as the IDF not only defeated the combined military forces of state adversaries on three geographical fronts simultaneously in 1967 and 1973, but it also conquered territory to more than double its own size in 1967.[14]

Lessons from the conventional battlespace that have been adopted into the cyber, subconventional, and nonconventional battlespaces are based on the distinction between three national situation levels in the context of which deterrence must be achieved and the defensive mode implemented. These are routine, emergency, and war. War is to be avoided as a single defeat may destroy the state. The defensive mode is routine. The daily routine is not to engage in combat. Compellence and preemption of offensive capabilities of the enemy in an emergency is an instrument for inducing deterrence (pre-terrence). To implement the defensive mode for these national situation levels in cyberspace, the IDF has adopted a comprehensive cybersecurity policy approach with a specific focus on developing cyber robustness, cyber resilience, and capacity.[15]

There is consistency for how this is achieved; cyber uses many of the same concepts as conventional tactics. This is with state-of-the-art technology and flexibility of equipment with an integration in the thinking, tactics, and strategy of the kinetic weapon (conventional) with cyber. Cyber equipment as with conventional equipment is procured, which enables switching between offensive and defensive modes. The cyber equipment, both hardware and software, is the same for the offensive and the defensive modes, and therefore training for the defensive also has the capacity for the offensive. Experience from the conventional battlespace, for example, is the Israeli Air Force that has invested in flexible weapon systems and multi-role combat aircraft capable of carrying out both offensive action—bombing enemy targets—and defensive missions—intercepting enemy aircraft in Israel's airspace.[16]

While the IDF has been less effective operationally in subconventional spaces than the interstate conventional wars, the experience and lessons learned from both have also been applied and implemented in cyber. For example, the subconventional battle threat is an asymmetrical confrontation where the outcome appears to demand a political solution rather than a military option. Whereas a single Israeli victory evident in the conventional wars could achieve deterrence against states, such single successes cannot settle the subconventional conflict against radicals and terrorist organizations.

In the subconventional conflict, counterinsurgency military campaigns, such as those in Gaza and Lebanon, have been limited in scope and duration as needed. Such counterinsurgency deployment in Southern Lebanon from 1982 to 2000 did not resolve terrorism coming from there. Public opinion and with it political action are against deploying IDF ground forces deep inside adversary territory for a sustained duration, as that would result in heavy casualties.[17]

Indicative of consistency, these experiences and lessons learned are extended into cyber. With the subconventional as it relates to cyber, it is accepted that any military option will not end the hostilities. Here a cyberattack is also a military attack as it is a weapon that can cause damage, and the response can similarly inflict damage and casualties. The routine then is the defensive mode and not offensive, not even cyber. As with the conventional and subconventional battle threats, the IDF approach to the cyber battle threat is not to engage in protracted conflict as routine. The projection of nonnuclear (conventional) deterrence is conveyed in cyber, as in the conventional and subconventional battle spaces, as the form of any attack will have a similar response.[18]

This is predicated on the role of compellence and preemption of offensive capabilities of the enemy as an instrument for inducing deterrence (preterrence). As with the subconventional, the IDF undertakes cyber offensives of specific targets for specific or limited purposes. The objective is a measure of active defense—preemptive or preventive strikes. For example, they could be part of DCO-RA operations, but as in the physical domains, caution is taken to assess the effects of countermeasures as they are limited and could typically only degrade, not defeat, an adversary's activities.[19]

Limited and Total Wars

The consistency in CMR with the defensive mode as routine starts with the political objective. The political objective determines the aim of combat or why the war is being fought. This provides an understanding of how the war is to be waged—the military implementation. Conceptually, this is evident in the distinction between two forms of war—limited and total—both politically and militarily. As defined, a *limited war* militarily is one where the belligerents do not expend all of the resources at their disposal. These could be human, industrial, agricultural, military, natural, technological, or otherwise and have specific targets and goals and time frames.[20]

In deciding on a limit for war, an assessment and evaluation of capability and capacity and the adversary themselves determines both politically and militarily the value of expending resources. Politically, Israel's subconventional adversaries are on international terrorist lists. Hamas has been on the United States Foreign Terrorist Organizations list since 1997.[21] Also, Hezbollah and Hamas are both on the European Union's terrorist list.[22] These cannot be targeted easily for they are barely distinguishable from the civilian populations they coexist with. Militarily then, even if the IDF used all the resources in Israel, there is no evidence to suggest that this would bring an end to hostilities. With this in mind, the IDF is in defensive mode as routine with offensive combat limited.

Conversely, Israel's subconventional adversaries do not function the same. For example, Hamas in Gaza and Hezbollah in Lebanon do not have an electorate to answer to, they do not recognize the right of the State of Israel to exist, and will not enter into any negotiations to end hostilities and conflict. Their regular use of violence and terror with all available resources at civil and military targets alike could well be considered as engaging in a total war against Israel.[23]

As defined militarily and politically, *total war* is where nothing and no one is exempt and includes any and all civilian-associated resources and infrastructure as legitimate military targets, mobilization of all of the resources of society to fight the war, and priority is given to warfare over noncombatant needs.[24] Both Hamas and Hezbollah meet this definition, attacking Israeli civilians, government, and military targets.

Furthermore, Iran is evident in all four battle spaces and threats. The potential conveyed in the *IDF Strategy Document* was "for an escalation in one battle space that could also be, or lead to, an escalation in others, especially if the adversaries were the same."[25] A scenario could be that Hamas and Hezbollah, being the proxy of Iran, and together with Iran, would act in unison and escalate in response to an IDF offensive in one of the battle spaces. As a routine then the IDF is in "defensive mode in cyber and rests on limited cyber offensive activities where cyber is locating equitably along other spaces of operation and threats."[26]

Limited Cyber Battle

The two main features distinguishing limited and total war are the use of resources and targets that could also determine the duration and intensity of the combat. In the CMR in all four battle spaces and threats, the IDF is limited by the political echelons in targeting both in its geographical and demographic jurisdictions.[27] In limiting these, the IDFs' roles and mission are defined and differentiate military with security. As the military, the IDF has a limited cyber battle in a defensive mode compared to that of the more comprehensive or total cyber battle of the security organizations that are in a more proactive offensive mode investigating, arresting, and prosecuting cyber criminals. A brief look at these differences explains this.

The geographical parameter for the IDF is the external defense of the State of Israel—that is, its borders. The IDF may be deployed within the state's borders in civil support (e.g., education) and in emergencies (e.g., earthquakes and medical support). If there is doubt, then the line is drawn when defining the target, namely the specific missions and roles of the IDF. The citizens of the state and other civilians are not normally a military target using any means, including cyber, both within the state or externally in other states.[28]

A distinction on the specific missions and roles of the IDF was evident when the then-Chief of the General Staff Lieutenant General Gadi Eizenkot did not mention other weaponized forms of warfare: information, psychological, and political warfare when he located cyber as the fourth of battle threats along other weapons and spaces of operation, namely land, sea, and air.[29] This could be explained, as for Eizenkot and his predecessors security is different to defense/military, and moreover the IDF does not target civilians, only military combatants.[30]

The various other actors in the Israeli security structures, such as the police, the Border Police (MAGAV מג"ב), and the Israeli Security Agency (ISA/Shin Bet/*shabak* שב"כ)—and not the IDF—are deployed within the state's borders investigating, targeting, arresting, and prosecuting civilians including the subconventional (terrorists) and cyber spaces and threats. Throughout Israel's history, it was these agencies and not the IDF that were the main operatives for the task of the psychological or information operations dealing with Palestinians within Israel's borders and governance area, including the West Bank, Gaza, and East Jerusalem.[31]

The security organizations and not the IDF handled Israel's propaganda and outreach targeting Palestinians during the 1956 and 1967 wars and psychological operations during the period of counterinfiltration operations against the Palestine Liberation Organization's (PLO) attempted infiltrations of terrorists from Jordan and Lebanon during the 1960s, 1970s, and 1980s, before adequate fencing was constructed to prevent these cross-border infiltrations.[32] The security organizations also handled the "winning the hearts and minds" psychological operations in the Second Intifada (2000–5).[33]

Another case is the anti-Israel cyber activists/hactivists, and these could also be mainly civilians and therefore outside of the targeting jurisdiction of the IDF. Such activism/hactivism is in the largely global and unregulated internet, or the cyber underworld, that provokes a response by pro-Israel cyber activists and the security establishment.[34]

Similarly, there is not exact data and information for an accurate analysis on the full extent of IDF units that operate in close cooperation and coordination with the security organizations, as the same radicals and terrorist organizations operate both from outside and within Israel. There are, however, known to be information, psychological, and political warfare units in the IDF, especially elements of IDF Intelligence Unit 8200.[35]

The Determination and Implementation of Civil-Military Relations

The laws of the State of Israel grant the democratically elected civilian government the ability to determine the political decisions relating to adversaries, while the IDF decides the military implementation. This process takes the form of a constant debate and discussion by the leaders in the civilian government and the leaders in the defense and security organizations, where this debate is the definition of civil-military relations (CMR). In the debate, the IDF is deemed the professional entity with the expertise and so advises the civilian government's decisions on what is viable militarily. It is the civilian government who weighs the options and makes the decision as to whether to use a military option.[36]

As cyber is one of the four battle spaces and threats along with conventional (state), subconventional (nonstate), and nonconventional, then it is fair to say that there is a cyber battle terrain and that cyber is a true type of weapon. In examining the IDFs' role in CMR to implement any decision taken by the civilian government, and given the consistency in CMR for all four in the defensive mode as routine, this section uses case studies to examine the specific cyber weapon with examples in four subsections: planning and preparation, authority and jurisdiction, fencing the battle terrain, and mapping the battle terrain.

Planning and Preparation

The IDF planning and preparation for routine, emergency, or war on any battle terrain have been with specific threats against Israel in mind. In 2021, these are from Iran and its nonstate proxies—Hamas in Gaza and Hezbollah in Lebanon. One aspect of such planning and preparation is based on scenarios. One scenario is the potential escalation from one battle space to an overall escalation in all four battle spaces, thereby making planning for all four battle threats extensions of each other.[37]

A specific scenario is the result of a cyberattack from any one of these adversaries, for example, hacking to falsify sensor signals in an electricity power station that would lead to physical damage of the power station and electricity outages. Citizens and the economy may face significant damage from this.[38]

Protecting and thwarting such an attack would be the responsibility of the electricity company, private expert cyber contractors, and the security organizations while the IDF would be tasked to collaborate in the provision of advice and intelligence. It is the specific role and mission of the IDF, if such an attack did take place by a combatant adversary such as Iran, Hamas, and Hezbollah, to implement a response. The IDF also needs to respond in a way that would not lead to an escalation and would also deter any further attacks. The severity and nature of such an attack and the responses required shows why cyber bears many similarities to other types of weapons and military attacks. A cyberattack using a cyber weapon "is an attempt to expose, alter, disable, destroy, steal, or gain access."[39]

Considering such a scenario, and given the potential for an escalation across all four battle spaces and threats with the same adversaries and the consistency in having to deter through a strong defensive posture, explains why IDF cyber capacity—both equipment and training—has been developed as part of its arsenal integrating cyber with other tactics, strategy, and weapons.[40]

Experience and lessons from the other battle spaces and threats have been applied to cyber. For example, conceptually, cyberspace is a space as are air and sea spaces. The IDFs' task is to plan and to prepare to control any space, especially where there may be a threat. The similarities also extend to procurement and training. Aircraft and ships may be flexible platforms for many various systems, both offensive and defensive.[41]

Computers as the hardware are also flexible platforms for different types of software. Basic training on information systems, infrastructures, computer networks, or even personal computer devices for the offensive mode is no different from that of the defensive. Specialist training is required and provided for the specific weapon system; in cyber, it is the software.[42]

Experience and lessons in the planning, preparing, procurement, and training from the navy and air force can be conceptually applied to cyber. As the four battle spaces and threats are on a continuum, there then could be symbiotic kinetic (conventional) and cyber efforts to achieve the same objectives of deterrence and defense.

An example of an IDF response to a Hamas cyberattack was not cyber but was an air strike on the building housing Hamas cyber attackers in 2019.[43] Other examples are DCO-RA operations where IDF cyber capabilities and electronic attacks suppressed Syrian air defense networks to enable Israeli Air Force jets to strike more than 500 targets in 2020, mainly arms transfers and supply routes, possibly from Iran to Hezbollah.[44]

Authority and Jurisdiction

The IDF in all four battle spaces as a routine is in the defensive mode, yet it has also planned and prepared to be operationally offensive. That stems from the basic universal principles that any state is entitled to defend its existence, including using armed force.[45]

There are at the same time important instances and circumstances that limits the propensity in CMR to grant the IDF the general authority and jurisdiction to implement preventive and preemptive strikes for immediate military response if attacked and to attack targets of opportunity. A prime reason is caution. An intelligence or other failure could lead to the wrong target being attacked with the consequence being an escalation that might extend beyond cyber and into a full conventional war. For example, the attacker could be an individual terrorist but operating from another country that spoofs their identity to another person in another country.[46]

The caution on escalation is explained by demography, geography, economics, and casualties. Israel has no geographical strategic depth; it cannot absorb an armed attack by adversarial conventional forces. Mobilization of reserves in an emergency for more than a month or two, and with physical damage to industry and commerce, would be at the expense of the economy. Probably the most significant factor that influences political decision makers is the potential for many casualties, both military and civilian. Most of the population lives in a narrow stretch of dense urban dwellings in the Jerusalem-Tel Aviv corridor and could be annihilated in any mass aerial attack.[47] Moreover, the IDF is a people's army. All the soldiers are citizens and all the citizens are soldiers. Casualties are the fathers or the sons in any family, or indeed daughters as women also have compulsory service. And citizens have grumbled and protested that the government and the IDF are not doing enough.[48]

Such existential considerations offer the essential explanation for the consistency in CMR through all four battle spaces and threats to limit the offensive mode. They offer justification to Israel's defense doctrine where any act that might escalate to war is a no-choice option, which carries a heavy social and economic price tag. Given the caution for escalation, cyber as a weapon and as a battle terrain is located firmly in this same doctrine that relies heavily on the projection of deterrence with the defensive mode as routine.[49]

Fencing the Battle Terrain

With the political option preferred over the military option in CMR, see the last interstate war in 1973 and peace treaties with Israel's southern neighbor Egypt (1977) and eastern neighbor Jordan (1994). The residual defense status quo of politically unresolved issues, for example the Palestinian question, sees consistent low-intensity terror and attacks from terror groups in the subconventional and cyber spaces. There are occasional escalations to counterinsurgency with limited campaigns, for example, in Gaza and Lebanon. The status quo is not one where there is any disagreement between the political and the military. The asymmetrical nature of these campaigns and their religious, ethnic, and territorial issues does not lead easily to a military option. Even extended operations to buffer from subconventional attacks (rockets) and working with proxy forces from 1982 to 2000 in Lebanon with the South Lebanese Army have not resolved the status quo.

This political status quo with an inability to have a decisive military solution leads to a consistency in CMR for the defensive mode for all four battle spaces and threats. The defensive mode is not just passive and waiting to repel an attack. The defensive mode has active characteristics and options that are evident when posing the question, "What is to be defended?" This discerns between active and passive defense and protection. Active defense may be DCO-

RA that when implemented could link kinetic (conventional) with cyber. For example, in 2007, the IDF employed cyber capabilities and electronic attacks to suppress an enemy air defense network so that Israeli Air Force jets could destroy a suspected nuclear facility in Syria.[50]

Protection is an example of the IDF defending the borders of the State of Israel using fencing. Throughout the 1950s and 1960s in the subconventional space and threat, Palestinian *Fedayeen* crossed into Israel from Egypt, Jordan, Lebanon, and Syria, attacking civilian and military targets. Progressively over decades, border fences were erected around local agriculture settlements and then cities and finally around the whole border of Israel. Israel aimed to have a closed land, sea, and air space.[51]

New and more formidable fences were progressively erected along the northern Lebanese border to prevent PLO incursions in the 1970s and 1980s.[52] Then a more sophisticated seven-mile long land berm (earth barrier) fence was constructed on the same border to defend against the Iranian-backed Hezbollah that replaced the PLO.[53] A wall has been constructed in the West Bank after the Second Intifada (civilian uprising that saw 171 suicide bombings).[54] Since 2005, fences have been erected to prevent Hamas incursions from Gaza on the southern border and then replaced with more sophisticated ones.[55]

Such fencing has progressively included cyber elements. In the fences and the wall, technology has played a role. In the 1960s, there were electric tripwire border fences, in the 1970s the fences were watched with closed-circuit television surveillance (CCTV), and by the 1990s drone surveillance. Now software programs reduce the need to have a human operator man the audio, visual, and infrared surveillance on a 24/7 basis. The automated systems can monitor Israel's border fencing and instantly alert forces on the ground, air, and sea of an incursion or a pending incursion. Or there could even be remotely controlled responses such as missiles from drones.[56]

As with territorial space, cyber is also a space that needs to be defended and protected. Computers and software are the weapons wielded by human hands and networked computing is the battle terrain space. The experience from the border fencing defensive concept of protecting Israel's territorial borders has reduced the frequency and intensity of attacks. It would not be innovative to suggest that cyber fencing is solely an IDF tactic or measure as it is used worldwide. And it is effective to a large extent.

The basic notion of cyber fencing is to have essential government and military computer infrastructure on a separate physical network from publicly accessible networks. This is not perfect, as with physical fencing's weaknesses there are also weaknesses in cyber fencing. For instance, wireless, satellite, and Wi-Fi communication with forces in the field could be intercepted and false data inserted. There are active measures such as encryption of data that could be taken to prevent this. Another weakness is when networks and software upgrades are provided from commercial providers that might have malware or viruses.[57]

Mapping the Battle Terrain

While fencing (protection) may reduce the frequency and intensity that the IDF engages in subconventional and cyber combat and also prevents civilian casualties and damage, it can serve to stress that neither the political nor military option are viable to negate and neutralize Israel's adversaries. The defensive mode is preferred, though in an emergency, threat reduction by targeting (active defensive) is another means in the military toolbox.

To implement threat reduction using targeting, the IDF is tasked with mapping the battle terrain. Once the adversary has been identified and located then they can be targeted. In the subconventional (conventional/kinetic) battlefield, the IDF has implemented pinpoint air strikes on adversaries' rocket launch sites, weapons arsenals, and terrorist camps and the occasional targeted assassination.

An example is when, on 12 November 2019 at 0400, Baha Abu al-Ata, a militant leader of the radical Palestine Islamic Jihad in Gaza, was targeted and assassinated by two missiles launched from an Israeli Air Force McDonnell Douglas F-15I Eagle aircraft.[58] In the planning and preparation of the assassination, there was collaboration and coordination in the sharing of data and analysis among and between many Israeli politicians, military leaders, military units, and different intelligence services and their units, including the IDF Units 504, 8200, and 9900 and the ISA/Shin Bet. Individuals involved in the decision making included the prime minister, Benjamin Netanyahu, who was also minister of defense at the time; the Security Cabinet; the ISA director; and the IDF chief of staff.[59]

Active defenses including targeting infrastructures and people fall under the definition of preventive or preemptive acts. The objective is to weaken and disable the adversary as far as possible for threat reduction but not to engage in a way that might escalate to a full-scale war.[60] Gaining the upper hand in the cyber battle terrain by targeting the attacker is no different to that of the kinetic battle terrain. The outcome of the mission is impacted by successful situational awareness or the mapping of the battle terrain. It is knowing the adversary's capabilities that determines successful threat reduction through targeting. In cyber, self-awareness of capabilities is essential in order to overcome the inherent advantages that an attacker might have. Two examples are anonymity or hiding in a global network across national sovereignty and jurisdiction boundaries and forensics or the volatile and transient nature of evidence of their location that complicates analysis.[61]

Resolving this also assists in determining the motive and so the response to a cyberattack, which might not be politically motivated even if the target is government or military. An attack could be by a seasoned criminal, a random malicious venture, or even a local citizen without prior malicious intent. Yet, a single cyberattack could cause strategic and even tangible security damage. The process of targeting is to confirm the attacker as a premeditated serial terrorist and to assess whether targeting would result in collateral damage.

Even when the attacker has been identified and confirmed as a member of a terrorist group and their location determined, it is not a foregone conclusion that targeting can be implemented. For example, in 2005 Israel implemented a unilateral withdrawal from Gaza. Hamas took the governance in an election but continued to use terror, launching rockets and incendiary balloons across the border. There was a dramatic increase of cyber hacking attempts and virus attacks by individuals in these groups, apparently only using personal computers linked to commercial internet providers by telephone modems. One option was for the IDF to have responded by destroying the buildings in Gaza, where some individuals were operating, but there was no guarantee that others would not have taken their place. Or that Hamas and its state sponsor Iran would not have escalated the conflict with rockets and missiles. This was an extension of the other battle spaces because Iran is the main financier, weapons provider, and ideological force behind Hamas in Gaza and Hezbollah in Lebanon. Therefore, the best solution for the IDF was the defensive mode.[62]

The catalyst that enabled the option for active defense and targeting came from successful cyber terrain mission mapping, digital surveillance, and monitoring. To actively defend a mission in cyberspace, efforts were taken to understand and document that mission's dependence on cyberspace and cyber assets. This is known as cyber terrain mission mapping. For example, nonstate groups in Gaza were detected in 2006 as working with the cyber warfare units of sovereign states, Syria, and Iran. It meant that for the first time the IDF could plan and prepare to implement cyber strategies against specific military cyber targets of significance in these states. The battle terrain was mapped for potential targets that would also be in proportionality to a cyberattack against Israel, as required by international laws and customs.

Although there was speculation in the media of both sides cyber attacking each other, there was no official data or confirmation. Normally, cyber warfare is conducted secretly and anonymously. There is no good reason to expose one's identity or claim or deny responsibility, as it would almost certainly result in a response. In most cyber cases, identifying the source of the attack is difficult, and so escalation is avoided. The attacker operates from afar, secretly, while defenders focus on securing the cyber space.[63] With this understanding of the risk of being identified and leading to an escalation, the IDF operates in the defensive mode in cyber.

The Organizational Infrastructure of Civil-Military Relations for the Cyber Battle Threat

There are three distinct periods in the evolving IDF cyber organizational infrastructure that when examined show how the cyber battle space and threat evolved to the significance of being assessed as equal to that of conventional, subconventional, and nonconventional. The first period was 1993–2003, the second period was 2004–13, and the third period was from 2014 to present. This section examines the periods that were concurrent with subconventional threat campaigns as well as peace processes.

The periods will be examined for a consistency in CMR for all four battle threats and for the tendency to use the defensive mode as routine and not to initiate in combat unless necessary, as political rather than military options are proffered by the civilian government and by extension of the process of CMR, also in the IDF. In the first two periods, there were the same two evaluations by the IDF: one on weaponized information and the other on cyber that confirmed this defensive mode. Events in 2014 were a catalyst to placing cyber on an equitable level with the other threats. In 2020, cyber plans, policies, preparations, training, tactics, and strategies were put to the test.

The First Period, 1993–2003

The first period evolved from the 1980s with the advent of computers in soldiers' homes connected by modems over telephone lines to the internet. There was a potential for damage from viruses infected from the internet and transferred by portable media, such as floppy disks, from their systems to the IDFs'. An example of two events highlights the threat. One of these was the global cyberattack in 1988 by Cornell University graduate student Robert Morris using the Morris Worm. Another was in 1993, when John Arquilla and David Ronfeldt, political scientists from the Rand Corporation, published an article "Cyberwar Is Coming!," which foresaw a deep change in the structure of military organizations, with the expected frequent occurrence of cyberattacks.[64]

The IDF undertook two evaluations to determine if the decades-old Israel-Arab conflict could become a digital or electronic battlefield.[65] The first was on weaponizing information. Between 1994 and 2003, there was no evidence to suggest that influencing Palestinian public opinion using propaganda, psychological warfare, information warfare, political warfare, or even disinformation would have any value on influencing Palestinian leadership.[66] At the same time, there was no evidence that Israel's adversaries would have any impact on the public opinion of Israeli citizens or soldiers, even during the Second Intifada.[67]

The second evaluation was concurrent and focused specifically on cyber, for example computer hardware devices, computing software, and computer networks. There was apprehension that in the cyber realm, known terrorists or even individual anarchists could cause substantial disarray and even damage. Israel, in conjunction with other countries, and in a partnership of government, military, and the private sector took to identifying any emerging challenges. A long list was compiled that included individuals hacking into bank computers, organized crime, and extremist terrorist groups—some state sponsored as well as rogue states.[68]

There was a real concern given the growing use of computerized equipment in the IDFs' control, command, communications, and intelligence units (C3I). The conclusion was that if cyberattacks were successful then data could be stolen, corrupted, altered, or destroyed. A virus could freeze IDF operations. Having identified and classified cyber as a weapon, for all intents and purposes, led in 1997 to the establishment of the "Tehila Project" (Government Infrastructure for the Internet Age). It worked with global partners to envisage scenarios and prepare to counter them.

The emphasis was on defending systems and in particular isolating them on a separate network not connected to publicly accessible networks, per se fencing protection, in the same military notion of the physical fencing of the state's borders that had been taken for conventional and subconventional purposes.[69]

One cyber threat scenario became reality in 2002 with the first significant global cyberattack. It was the targeting of 13 domain name system (DNS) root servers around the world, in a distributed denial-of-service attack (DDoS), which assaulted the entire internet with a flood of data and slowed it down to a stop. Email was not delivered and websites could not be opened.[70]

Defending against cyber threats following this DDoS attack in 2002 were classified on the level of countering serious terror events. It led to the establishment of the Israeli Information Security National Authority (ISNA) within the Israel Security Agency. It was tasked with gathering information and supplying professional guidance on computing and computer infrastructure security to both the private and the public sectors to protect against threats of crime, terrorism, espionage, and exposure.

Working with the IDF, the ISNA identified one highly prioritized threat to the kinetic military forces. That was the vulnerability of computer-aided navigation and early warning systems (EWS) integrated into computerized platforms. These rely on precise satellite-based global positioning system (GPS) and timing. The serious joke went as follows: "Question: How can the enemy destroy an entire squadron of F-15 aircraft? Answer: By hacking into the airborne refueling aircraft and changing its GPS location—it won't find the squadron, no refuel, and the F-15s will fly into the sea." The solution was technologically akin to defensive protection. The Israel Aerospace Industries (IAI) developed an advanced GPS antijamming navigation system to defend against GPS-denying systems that block communication between aircraft and satellites.[71]

The Second Period, 2004–2013

In 2004, a newer generation of IDF generals undertook new evaluations of the same two topics: weaponized information and cyber, for example computer hardware devices, computing software, and computer networks. The adversaries were the same, but technology was evolving. In part, the evaluation on weaponized information was also instigated by the sign of the times of the American military engagement in Iraq with its "winning the hearts and minds" psychological operations.

The IDF found that effectiveness of weaponized information as being limited as it would not bring an end to hostilities in the asymmetrical confrontation in the subconventional battle space and threat against terrorist groups such as Hamas and Hezbollah. Nevertheless, the Operations Branch of the IDF general staff opened experimentally the Center for Consciousness Operations (*Malat* מל"ת) at the end of the Second Intifada in 2004. It reported to the Operations Branch (in terms of command) and to the Military Intelligence Directorate (from a professional perspective).[72] The initial intent of the creation of Malat was to support kinetic operations in times of emergency and war. It became operational for this purpose in the Second Lebanon War (2006) but had very little functionality as there was a lack of preconceived plans.[73]

Part of the evaluation on weaponized information entailed examining cooperation with the various security organizations, such as the police, MAGAV, and ISA on the growing popularity of social media. During this period was the advent of Facebook in 2004, Twitter in 2006, and Instagram in 2010. It was found that social media could increase the fog of war; for instance, during an asymmetrical conflict where civilians could be motivated into civil unrest and demonstrations where they lived in the same buildings in Gaza as terrorists who did not wear uniforms, thereby making it hard to ascertain who was a combatant and hence respond with military force.

Radicalized individuals and groups could also use such social media across international borders in an attempt to change civilians' opinions and motivate them to take militant action. This could have led to an escalation involving Muslim populations within Israeli cities. Although it did not happen, a scenario entailed blocking social media as it would not have been possible to effectively manage cyber social battles, especially as disinformation could be conveyed and widely distributed.

Such disinformation could also have had an effect on IDF soldiers' morale as they were also using social media. The best solution determined was to warn

Israeli citizens and soldiers not to rely on information provided by social media and not to provide information on themselves that could cause harm and damage, in the same manner that the average person would not advertise their credit card number.[74]

On the basis of these evaluations, the use of the Malat unit was put to test in Operation Cast Lead in October 2008 in Gaza, which was a limited military campaign as an extension of counterinsurgency. This would be the first time that the IDF embarked on a combat venture with the preconceived plan to have a psychological warfare (PSYWAR) component in coordination with the tactical forces. Malat found that PSYWAR in its own right had little value as there was no evidence to suggest that influencing Gaza residents using propaganda, psychological warfare, information warfare, political warfare, or even disinformation would have any value on influencing Palestinian leadership. Conversely, it could impact the success of kinetic operations by delivering specific messages to certain Hamas fighters and units broadcast using different types of media. After the operation, when the kinetic forces returned to base, so did the psychological warfare unit.[75]

The takeaway from this was that it was possible to communicate directly with individual adversaries. However, in a reciprocal manner, it was also possible for the adversaries to communicate directly with Israeli citizens and IDF soldiers and to steal data from their computerized devices that were using the internet. For instance, fourth-generation cell phones and tablets met this description and were added to the list of desktop computers and laptops that posed an increased cyber threat to the IDF. Soldier's movements could be tracked if the cell phone's systems were hacked, for example. This was hard to resolve and tackle as every soldier on every base and every citizen, maybe from the age of four, were using cyberspace in all aspects of life, including banking, education, booking travel, ordering takeout food, and watching news channels. Clearly it had become impossible to separate the daily life of the whole country from the cyber life of physical computerized devices and computerized networks, and it blurred the distinctions between the software and applications, including social media applications and the delivery of weaponized information and propaganda.

To ensure both active and passive defensive measures, a National Cyber Initiative was set in motion and led in August 2011 to the establishment of a National Cyber Bureau in the Prime Minister's Office. Being located within the top level of the political hierarchy, it was intended to be a coordinating bureau or "strategic roof" for all relevant cyber and weaponized information affairs. Data on potential critical threats could pass up to it from many organizations, be evaluated, and if needed shared with others throughout government. For example, if a threat was identified and had economic implications then all parts of government working in trade, industry, and commerce could be informed to improve national preparedness.[76]

In the IDF, enhanced cyber units were established to enable it to implement participation with the various security organizations. None of these units had an offensive mode as a routine task for cyber operations against any adversary. Their main task was gathering data, analysis, and protection. For example, the IDF Cyber Bureau was created within Unit 8200, one of the three main units in Intelligence (*aman* אמ"ן) and is responsible for collecting signal intelligence and code decryption. It works with Unit *Hatzav* (חצב), which collects open-source intelligence, including radio, television, newspapers, the internet, listening posts in Israeli embassies abroad, information from the tapping of undersea cables, and Gulfstream jets with electronic surveillance equipment. A Cyber Defense Department was also created within the command, control, communications, computers and intelligence (C4I) Directorate "tasked to thwart intelligence attacks and prevent disruptions and damage to components of the IDF's [*sic*] computing system, doctrinally defined as security comparable to the securing of IDF bases."[77]

To be sure the evolution of technology has meant that *command and control* (C2), a term used in the military around the world before computing has progressively had more added to the extent that it is now C6ISR—command, control, communications, computers, cyber defense, combat systems and intelligence, surveillance, and reconnaissance (ISR).

The Third Period, 2014–Present

In 2014, two events led to cyber being reexamined and reassessed and then elevated to be equal to the conventional, subconventional, and nonconventional battle spaces and threats. This was both reactive and proactive to ensure that cyber would be granted the due attention in recognition of its threat level.

The first was Operation Protective Edge in Gaza, a limited subconventional military campaign to combat counterinsurgency against Hamas in July.[78] The second event was the deteriorating relationship between the Israeli prime minister Benjamin Netanyahu and the American president Barack H. Obama over the Joint Comprehensive Plan of Action, known more commonly as the Iran nuclear deal. In Israel's view, it was not a good deal to prevent Iran from attaining nuclear capability and so posed a potential nonconventional threat. The IDF saw all the threats and battle spaces being intricately linked as Hamas was Iran's proxy and both were increasingly engaged in cyberattacks. There was the perceived necessity for IDF enhanced cyber preparedness to supplement and complement similar preparedness in the physical battle spaces as an escalation in one could lead to an escalation in all.[79]

This led Prime Minister Netanyahu to announce in 2014 that "I have decided to establish a national authority for cyber affairs, which will take care of the cyber defense of Israel. Not only for the defense of important installations and defense facilities, but also to protect the citizens of Israel from attacks."[80] The role and mission of the National Cyber Security Authority as the executive arm of the National Cyber Bureau would be to "evaluate and to formulate defensive responses to cyberattacks, including the handling of cyber events in real time, but wouldn't per se engage in any offensive operations."[81]

The wording had an emphasis on defense, indicating the political echelons saw a continuum in the defensive mode that was extended in consistency in CMR to the IDF who created a separate cyber branch to consolidate all of Israel's cyber capabilities.[82] Both the IDF and security organizations would work together with private contractors, some of whom had served as conscripts in IDF cyber units or similarly in the security organizations. For example, Israel Aerospace Industries created an online cyber academy to train on a cyber security simulator, the TAME Range Trainer. A broad range of cyber security scenarios are simulated and accompanied by exercises, lessons, and field implementations that provide trainees a real-time picture of the nature of the attack.[83]

The chief of the General Staff of the IDF, Eizenkot, confirmed the new status of cyberspace and threats as being significant and equal to the others and as being a continuum of them in CMR with a preference to the defensive mode as routine in two publications. The first was in the 2015 *IDFs' Strategy Document* that informed of the IDFs' engagement in planning, preparation, training, and defense to meet all threats including cyber where an "escalation in one battle space could also be, or lead to, an escalation in others, especially if the adversaries were the same."[84]

The second publication in 2018 was an article authored and published by Eizenkot, where he located "cyber as the fourth of battle threats along other weapons and spaces of operation, namely land, sea, and air. The three other battle threats are conventional (state), sub-conventional (non-state) and non-conventional."[85]

The first known and significant instance of the IDFs' cyber planning, policies, equipment, training, tactics, and strategy were put to the test was in 2020. This may be attributable to the success of the defensive mode where for years no significant attack was successful. In any conflict, an attack on essential civilian infrastructures is considered a serious and maybe existential event. Israel awoke to the news on 24 April 2020 that it was under cyberattack at several points against the national water system and attributed it to Iran, though it was not confirmed by them.[86]

For the first known time, in direct response to a state-based cyberattack assumed to be Iran, the IDF responded with a cyberattack against infrastructure at the Iranian port in Bandar Abbas on 9 May 2020 and declared that it was the IDF attack.[87] This was in direct response to Israel's national water system having had been attacked on 24 April and attributed it to Iran. The target was proportional and appropriate to convey a deterrent message that if critical infrastructure is attacked, Israel will respond in kind.[88]

This exchange of cyber fire was exactly that, and it served as a warning shot that a cyberattack on essential infrastructure would be reciprocated. To ensure that the message was being conveyed, Eizenkot's successor as chief of the General Staff of the IDF, Lieutenant General Aviv Kochavi, announced on 19 May 2020 that the IDF "will continue using a variety of military tools and unique combat methods to harm the enemy."[89]

Such a statement served to bring the attack and counterattack into public mass media focus and attention, a rare occurrence for cyber. In doing so, Israel woke up on 21 May 2020 with tens of thousands of mostly unsecured Israeli websites attacked, allegedly by Iran-based hackers, who disabled the sites and replaced them with a threatening message.[90] On 28 May 2020, Yigal Unna, the head of the Israel National Cyber Directorate, defined the situation as a "turning point" in the history of Israel's cyber warfare.[91]

Conclusions

What lessons could be taken away from the hypothesis and case studies? The hypothesis is that there is consistency of CMR in Israel. It is the same democratically elected civilian leadership that determines who are the adversaries and why. It is the same IDF that implements the decision of the civilian government when the military option is made as a process and procedure of CMR. The security concept has three basic pillars: deterrence, early warning, and decisive defeat. The broad purpose of Israel's strategy is the deterrence of aggression and the clear-cut defeat of the enemy if deterrence fails. There are three national situation levels: routine, emergency, and war. The case examined cyber as the fourth battle space and threat with conventional (state), subconventional (nonstate), and nonconventional. The four coexist with cyber on an equal level with air, land, and sea against the same adversaries. All are spaces that need to be defended and controlled.

In setting the case studies to the hypothesis, the evidence examined indicated a democratically elected civilian government consistency to prefer and determine political rather than military solutions. This was extended in CMR for the IDF to implement a defensive mode as routine and not to initiate combat unless necessary, for at the forefront of decision making were considerations of casualties. Influencing both political and military decisions in the process and procedures of the civil-military relations—that is, the debate on how to tackle the adversary—was an inability to successfully confront adversaries asymmetrically when using the military option. The IDF, with the professional military expertise, noted that this was both in the subconventional and cyber spaces as the adversaries were the same radical and extremist nonstate groups and terrorists. If the military option was used as an offensive, there was also the potential of an escalation from one battle space and threat that could lead to an overall escalation in all. In the process of evaluations and the debate between the civilian government and military, cyber was examined as part of the overall battle terrain and found to be equitable to others as a weapon.

No further gains could be achieved by using the full resources of Israel and the IDF, so the status quo was one of a limited war both politically and militarily as defined. It would be fair to say then that the IDF is engaged as routine in a defensive mode. The IDF is only engaged in a limited offensive mode in an emergency or an escalation to counterinsurgency in battles and war. Tactics include fencing, active defense, and preventive and preemptive actions. The IDF in general does not attack. It is normally defending, protecting, and deterring. This is the routine of the IDF.

However, the adversaries do not share the same policies with regular terror and cyberattacks against civilian, government, and military targets and using as much of their resources as possible. It would be fair to say then that they are engaged in the offensive mode in a total war.

It is also fair to say that this is now under trial. The status quo cannot be maintained eternally. A trajectory of events from the 2020 exchange of cyber fire with Iran questions whether cyber can bring any substantial gain that other weapon systems cannot. It questions whether using cyber to neutralize the pending nonconventional threat from Iran will lead to escalation. If not and if the IDF succeeds, then it might also assist in threat reduction and mitigating the subconventional threat from Iran's proxies Hamas and Hezbollah. The takeaway lesson could be that cyber as a weapon may demonstrate that nothing is set in stone.

The article concludes by noting its contribution to military studies. It has provided a hypothesis that has been examined and sustained in a case revealing new information and innovative analysis. Further research can build on the hypothesis proposed in this article. Further research can look at other cases to see if they are also applicable, such as a comparative study of cases to construct theories and paradigms and to build knowledge to enhance the study and understanding of cyber. These activities could contest this hypothesis or even offer a different one.

Endnotes

1. Yoav Zitun, "IDF Establishes New Cyber Branch," *Ynet News*, 28 June 2015.

2. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document] (Tel Aviv: Israel Defense Forces, 2015).
3. Meir Finkel, "IDF Strategy Documents, 2002–2018: On Processes, Chiefs of Staff, and the IDF," *Strategic Assessment* 23, no. 4 (October 2020): 4.
4. Gadi Eizenkot, "Cyberspace and the Israel Defense Forces," *Cyber, Intelligence, and Security* 2, no. 3 (December 2018): 99–104.
5. Finkel, "IDF Strategy Documents, 2002–2018," 5.
6. Raymond Horricks and Eyal Ben-Ari, *Military, State, and Society in Israel: Theoretical and Comparative Perspectives* (London: Routledge, 2018), 79.
7. Israel Tal, *National Security: The Israeli Experience* (New York: Praeger Security International, 2000), 67–88.
8. Yossi Arazi and Gal Perel, "Integrating Technologies to Protect the Home Front against Ballistic Threats and Cruise Missiles," *Military and Strategic Affairs* 5, no. 3 (December 2013): 94.
9. *Department of Defense Dictionary of Military and Associated Terms* (Washington DC: Department of Defense, 2019), 65.
10. Brian K. Chappell, *State Responses to Nuclear Proliferation: The Differential Effects of Threat Perception* (London: Springer, 2021), 198.
11. חטיבת כוח אדם [Manpower Division] (Tel Aviv: Israel Defense Forces, 2020).
12. מגזין "מערכות" צבא ההגנה לישראל, מהדורה מיוחדת: מלחמת אזרחים בסוריה [Maarachot Magazine Israel Defense Forces, Special Edition: Civil War in Syria] (Tel Aviv: Israel Defense Forces, 2020).
13. Shmuel Bar, "Israeli Strategic Deterrence Doctrine and Practice," *Comparative Strategy* 39, no. 4 (September 2020): 321–53, https://doi.org/10.1080/01495933.2020.1772624.
14. Ahron Bregman, *Israel's Wars: A History Since 1947* (London: Routledge, 2002), 20.
15. Jasper Frei, *Israel's National Cybersecurity and Cyberdefense Posture* (Zurich, Switzerland: ETH, 2020), 5.
16. Prime Minister Ehud Olmert's pronouncement that "a state cannot protect itself ad-infinitum," reported by Hana Levi Julian, "Olmert: A State Cannot Protect Itself Ad Infinitum," *Arutz Sheva News*, 29 June 2007.
17. Yaakov Amidror, *Winning Counterinsurgency War: The Israeli Experience* (Jerusalem: Jerusalem Center for Public Affairs, 2008), 16–18.
18. Dmitry Adamsky, "From Israel with Deterrence: Strategic Culture, Intra-war Coercion and Brute Force," *Security Studies* 26, no. 1 (April 2017): 57–184, https://doi.org/10.1080/09636412.2017.1243923.
19. *Department of Defense Dictionary of Military and Associated Terms*.
20. *Department of Defense Dictionary of Military and Associated Terms*.
21. "Foreign Terrorist Organizations," U.S. Department of State, accessed 23 March 2021.
22. "Council Decision (CFSP) 2020/1132 of 30 July 2020 Updating the List of Persons, Groups and Entities Subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the Application of Apecific Measures to Combat Terrorism, and Repealing Decision (CFSP) 2020/20," *Official Journal of the European Union*.
23. *Hearing Before the Subcommittee on Near Eastern and South and Central Asian Affairs of the Committee on Foreign Relations*, 111th Cong. (8 June 2010) (assessing the strength of Hezbollah).
24. Paul K. Saint-Amour, "On the Partiality of Total War," *Critical Inquiry* 40, no. 2 (Winter 2014): 420–49, https://doi.org/10.1086/674121.
25. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document].
26. Eizenkot, "Cyberspace and the Israel Defense Forces," 99–104.
27. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document].
28. אסטרטגיית צה"ל [Israel Defense Forces' Strategy Document].
29. Eizenkot, "Cyberspace and the Israel Defense Forces," 99–104.
30. Interview with MajGen Shlomo Gazit, former head of the Military Intelligence Directorate, at the Institute for National Security Studies, Tel Aviv, Israel, 12 December 2013, hereafter Gazit interview.

31. Elia Zureik, David Lyon, and Yasmeen Abu-Laban, eds., *Surveillance and Control in Israel/Palestine: Population, Territory and Power* (New York: Routledge, 2010), 161.
32. Padraig O'Malley, *The Two-State Delusion: Israel and Palestine—A Tale of Two Narratives* (New York: Viking, 2015), 18, 28.
33. Nachman Shai, *Hearts and Minds: Israel and the Battle for Public Opinion* (Albany: State University of New York Press, 2018).
34. Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford, UK: Oxford University Press, 2018), 168, https://doi.org/10.1093/acprof:oso/9780190204792.001.0001.
35. Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* (Tel Aviv, Israel: Institute for National Security Studies, 2016), 12–15.
36. Yehuda Ben-Meir, *Civil-Military Relations in Israel* (New York: Columbia University Press, 1995), 6–11.
37. Charles D. Freilich, *Israeli National Security: A New Strategy for an Era of Change* (Oxford, UK: Oxford University Press, 2018), 86, https://doi.org/10.1093/oso/9780190602932.001.0001.
38. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* (Idaho Falls, ID: Mission Support Center, Idaho National Laboratory, 2016), 4.
39. Andrew R. Wilson and M. L. Perry, eds., *War, Virtual War and Society: The Challenge to Communities* (New York: Rodopi, 2008), 192.
40. Lior Tabansky and Isaac Ben Israel, *Cybersecurity in Israel* (New York: Springer, 2015), 3, https://doi.org/10.1007/978-3-319-18986-4.
41. Frei, *Israel's National Cybersecurity and Cyberdefense Posture*, 34–36.
42. Paul J. Springer, ed., *Encyclopedia of Cyber Warfare* (New York: Springer, 2017), 158.
43. Zak Doffman, "Israel Responds to Cyber Attack with Air Strike on Cyber Attackers," *Forbes*, 6 May 2019, 12.
44. Suleiman Al-Khalidi, "Israel Launches Major Air Strikes on Iran-linked Targets in Syria," Reuters, 13 January 2021.
45. Ariel Levite, *Offense and Defense in Israeli Military Doctrine* (London: Routledge, 2019), 9.
46. Sharon Afek, "Breaking the Rules and Changing the Game: When Cyberspace Meets International Law," *Dado Center Journal*, no. 3 (December 2014): 43–72.
47. Yoav Ben-Horin and Barry Posen, *Israel's Strategic Doctrine* (Santa Monica, CA: Rand, 1981), v.
48. Gazit interview.
49. Shmuel Bar, "Israeli Strategic Deterrence Doctrine and Practice," *Comparative Strategy* 39, no. 4 (September 2020): 321–53, https://doi.org/10.1080/01495933.2020.1772624.
50. Chappell, *State Responses to Nuclear Proliferation*, 198.
51. Yehoshafat Harkabi, *Fedayeen Action and Arab Strategy* (London: Institute for Strategic Studies, 1968), 20.
52. Amos Gilboa, *The Threat of PLO Terrorism* (Jerusalem: Ministry of Foreign Affairs, 1985), 12–18.
53. Said Saddiki, *Israel and the Fencing Policy: A Barrier on Every Seam Line* (Doha, Qatar: Arab Center for Research and Policy Studies, 2013), 19.
54. Shaul E. Cohen, "Israel's West Bank Barrier: An Impediment to Peace?," *Geographical Review* 96, no. 4 (October 2006): 682–95, https://doi.org/10.1111/j.1931-0846.2006.tb00522.x.
55. Nejc Kardel, ed., *Israel vs. Hamas: The Middle East in Turmoil* (New York: Nova Science Pub, 2010), 28.
56. Mitchell Bard, "West Bank, Gaza and Lebanon Security Barriers: Background & Overview," Jewish Virtual Library, accessed 5 April 2021.
57. Amitai Gilad, Eyal Pecht, and Asher Tishler, "Intelligence, Cyberspace, and National Security," *Defence and Peace Economics* 32, no. 1 (January 2021): 18–25, https://doi.org/10.1080/10242694.2020.1778966.

58. “Israel Kills Top Palestinian Islamic Jihad Militant in Gaza,” BBC News, 12 November 2019.
59. Benjamin Netanyahu, “Netanyahu’s Remarks at a Press Conference in a Joint Statement with IDF Chief-of-Staff Lt.-Gen. Aviv Kochavi and ISA Director Nadav Argaman at the Defense Ministry in Tel Aviv,” Israel.org, video news conference, 12 November 2020.
60. Ehud Eilam, *Israel’s Military Doctrine* (Lanham, MD: Lexington Books, 2018), 9.
61. Alexander Kott, Norbou Buchler, and Kristin E. Schaefer, *Kinetic and Cyber* (Adelphi, MD: U.S. Army Research Laboratory, 2015), 4–5.
62. פיקוד כוחות היבשה, פעולות כוחות היבשה [Ground Forces Command, Ground Forces Operations] (Tel Aviv: Israel Defense Forces, 2012), 5.
63. International Institute for Strategic Studies, *Iran’s Networks of Influence in the Middle East* (London: Routledge, 2020), 27.
64. John Arquilla and David Ronfeldt, “Cyberwar Is Coming!,” *Comparative Strategy* 12, no. 2 (1993) 141–65, https://doi.org/10.1080/01495939308402915.
65. Khalid Walid Mahmoud, *Cyber Attacks: The Electronic Battlefield* (Doha, Qatar: Arab Center for Research and Policy Studies, 2013), 18–23.
66. David Jaeger et al., “The Struggle for Palestinian Hearts and Minds: Violence and Public Opinion in the Second Intifada,” *Journal of Public Economics* 96, nos. 3–4 (April 2012): 354–68.
67. Jacob Shamir and Khalil Shikaki, *Palestinian and Israeli Public Opinion: The Public Imperative in the Second Intifada* (Bloomington: Indiana University Press, 2010), 16.
68. IBP, *Israel Internet, E-Commerce Investment and Business Guide: Strategic Information, Regulations, Opportunities* (London: Lulucom, 2007), 89–92.
69. Israel Accountant-General Office, *Aspects of “TEHILA” Project Management* (Jerusalem: Ministry of Finance, 1999), 1–10.
70. Marian Quigley, *Encyclopedia of Information Ethics and Security* (New Delhi, India: Idea Group, 2007), 128.
71. Arie Egozi, “How Israel Is Leading the Global Cyberwarfare Race,” Defence iQ, 1 May 2019.
72. Amos Harel, “IDF Reviving Psychological Warfare Unit,” *Haaretz News*, 25 January 2005.
73. Adib Farhadi, *Countering Violent Extremism by Winning Hearts and Minds* (New York: Springer, 2020), 45–47, https://doi.org/10.1007/978-3-030-50057-3.
74. David Siman-Tov and Ofer Fridman, “A Rose by Any Other Name?: Strategic Communications in Israel,” *Defence Strategic Communications*, no. 8 (Spring 2020): 17–52, 30.
75. Ron Schleifer, הלוחמה הפסיכולוגית ב"עופרת יצוקה [Psychological Warfare during “Cast Lead”], *Maarachot Magazine Israel Defense Forces*, no. 432 (2010).
76. Michael Raska, *Military Innovation in Small States Creating a Reverse Asymmetry* (London: Routledge, 2016), 89.
77. Dov Alfon, *Unit 8200* [In German] (Hamburg, Germany: Rowohlt Taschenbuch, 2019), 28–32.
78. Daniel Cohen and Danielle Levin, “Cyber Infiltration During Operation Protective Edge,” *Forbes*, 12 August 2014.
79. Gil Baram, ההיערכות למלחמה קיברנטית [Cyber War Preparedness], *Maarachot Magazine Israel Defense Forces*, no. 456 (2014).
80. Moti Bassok, נתניהו: תוקם רשות לאומית להגנה אופרטיבית בסייבר [Netanyahu: National Cyber Defense Authority to be Established], *Marker*, 4 September 2014, 2.
81. Roni Katzir, “Government of Israel, Cabinet Decision 2444, February 15, 2015,” *Dado Center Journal*, no. 4 (2015): 117–35.
82. Yoav Zitun, “IDF Establishes New Cyber Branch,” *Ynet News*, 28 June 2015.
83. Shoshana Solomon, “Israel’s IAI to Help Bosnia Boost Cybersecurity Via Online Training Program,” *Times of Israel*, 30 September 2020.
84. אסטרטגיית צה"ל [Israel Defense Forces’ Strategy Document].
85. Eizenkot, “Cyberspace and the Israel Defense Forces,” 99–104.

86. Omree Wechsler, *The April Cyber-attack on Israel's Water Facilities* (Tel Aviv, Israel: Yuval Ne'eman Workshop for Science, Technology and Security in Tel Aviv University, 2020), 1–3.
87. Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility," *Washington Post*, 18 May 2020.
88. Warrick and Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility."
89. Lilach Shoval, "IDF Chief: Israel Uses Wide Range of Tools to Defend Itself," *Israel Hayom News*, 20 May 2020, 3.
90. "Thousands of Israeli Websites Down after Suspected Massive Iranian Cyberattack," CTECH, 21 May 2020.
91. "Israeli Cyber Chief Warns of 'New Era' in Cyber Warfare," Arutz Sheva News, 28 May 2020.

Russian Cyber Information Warfare
International Distribution and Domestic Control

Lev Topor, PhD, and Alexander Tabachnik, PhD

Abstract: Cyber information warfare (IW) is a double-edged sword. States use IW to shape the hearts and minds of foreign societies and policy makers. However, states are also prone to foreign influence through IW. This assumption applies mainly to liberal democratic societies. The question examined in this article is how Russia uses IW on other countries but protects itself from the same activities. The authors' main argument is that while Russia executes influence operations and IW in cyberspace, it strives for uncompromising control over its domestic cyberspace, thus restricting undesirable informational influence over its population.

Keywords: cyber warfare, information warfare, IW, Russia, cyber policy, sharp power

Introduction

Cyber information warfare (IW) is a double-edged sword. On the one hand, states can use IW to shape the mindset of foreign societies and policy makers. On the other hand, states are also prone to foreign influence through IW. This applies mainly to liberal democratic societies such as the United States, Britain, and most of Western Europe. Russia is a distinct case in this regard as it is a nondemocratic state that uses *sharp power*—it takes advantage of the asymmetry between open and democratic political systems and restricted nondemocratic political systems.[1] In an open society, freedom of speech and freedom of the press can facilitate disinformation and misinforma-

Dr. Lev Topor is a senior research fellow at the Center for Cyber, Law and Policy, University of Haifa, Israel. Dr. Alexander Tabachnik is also a senior research fellow at the Center for Cyber, Law and Policy.

https://doi.org/10.21140/mcuj.20211201005

tion while restricted political systems where speech and press are limited can restrict intervention through IW.[2]

The question examined in this article is how Russia uses IW on other countries in the international arena but protects itself from it. The article's argument is that while Russia executes influence operations and IW using cyberspace, it strives for uncompromising control over its domestic cyberspace, thus restricting undesirable informational influence over its population. Moreover, as Daria Litvinova suggests, Russia not only restricts its media and communication systems but, simultaneously, manipulates these systems for political control. The vast majority of Russian citizens consume state-sponsored media and news that promote pro-Kremlin narratives.[3]

As discovered in the case of the Russian intervention in the Scandinavian, East-Central European, and Baltic states since 2017, Russia's bots and trolls are very effective in negatively impacting Western democracies. Russia undermines the democratic nature of its adversaries, dividing their societies between competing groups—supporters of the right and supporters of the left, liberals and conservatives, and even racial divisions. In fact, any social rift can be used to divide and incite. Therefore, divisions created or amplified harm the governance of Russia's adversaries. In Russia's domestic arena, however, legislation is used strategically to ensure domestic obedience. For instance, the Yarovaya Law, which was enacted in 2016 alongside other laws and policies regarding its sovereign internet, allows Russia to restrict the flow of undesirable information. Moscow is obligated to supervise information even at the expense of the civil right for privacy, growing criticism from its domestic telecommunication companies, from other information technology (IT) giants, and despite substantial economic and reputational losses.

From Soviet Hard Power to Russian Sophisticated Information Warfare

The dissolution of the Soviet Union occurred on 26 December 1991. The Cold War ended with an ideational and material collapse as the Soviet Union could not compete with American and Western progress, mainly in economic and technological areas. Furthermore, the Soviet authorities failed to establish a unifying ideology as each ethnic group had different national narratives, needs, and privileges.[4] The military and economic power of the United States, along with its appealing competing ideology, slowly influenced the Soviet people and mainly the Soviet elite.[5] Though there are numerous explanations for the collapse of the Soviet Union, it is unquestionable that the American and Western combination of hard power and soft power superiority pushed the Soviet Union to its limit.[6] Ernest J. Wilson III and Joseph S. Nye Jr. regard this combination of power types as smart power. *Smart power* is the capability to combine hard and soft power in an effective way to amplify one's influence on others.[7] The Soviet Union did employ soft power such as economic pressure and propaganda, mainly on less developed countries but could not compete with Western diplomacy and economic power. Indeed, the Soviet Union mainly leaned on hard power for its international affairs and policies.[8]

Russia now makes use of sharp power with cyber influence operations and hybrid warfare.[9] In the last two decades, Russia emerged again and began to recover. In the twenty-first century, instead of fighting hard power with hard power, Russia uses smart power and information warfare to achieve its strategic objectives.[10] Since the end of the Cold War, a state of uncertainty was generated regarding American and Russian relations. The Cold War was over but struggle and competition for global primacy remained.

In Western terms, Russia employed *hybrid warfare*, which, as Timothy McCulloh and Richard Johnson define, is the generation of an uncertain situation between adversaries where it is unclear whether a state of war exists, and it is unclear who is a combatant and who is not.[11] Indeed, Russia used hybrid strategies and tactics in some cases, as in the case of Eastern Ukraine and Crimea. For example, it wielded irregular fighters, proxy fighters, and information and psychological warfare along with economic and diplomatic pressure to justify its actions.[12]

However, IW is not just a part of hybrid warfare, but it is a stand-alone strategy to promote policies and strategies to pressure one's adversary without the use of brute force. These strategies and tactics are not new and were frequently used by the Soviet Union. The Soviet, or Russian, term for IW is *active measures*—covert and overt techniques to influence events and behaviors of foreign countries. In these cases, information was manipulated and promoted by Soviet-supporting front organizations, agents of influence such as local politicians or even spies, by fake stories, and forgeries in non-Soviet media outlets.[13]

In the twenty-first century, for instance, the U.S. Global Engagement Center (GEC) issued a report in August 2020, stating that Russia has created a sophisticated "ecosystem" of propaganda outlets via official and unofficial channels like news agencies, websites, or social media bots and trolls. The actual impact of this ecosystem is yet to be clear as measuring information, influence, and reach is complex and inaccurate. Yet, this ecosystem does create a certain amount of debate, hostility among parties, and instability within the targeted state.[14] As it seems, the Russian ecosystem is an iteration of Soviet disinformation campaigns, in particular Soviet active measures.

Moreover, Russia uses IW as a complementary power to fit alongside other types of power. In a document issued by the Russian Federation Council titled "The Concept of the Cyber Security Strategy of the Russian Federation," Russia has emphasized the importance of cyber warfare, information and communication technologies (ICT), and use of cyber-related actions to accommodate and complement other types of acts in the international arena such as hard or soft power.[15] However, Russian security officials do not use the term cyber warfare. Instead, they conceptualize cyber warfare within the broader framework of information warfare and perceive it as a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations.[16]

Traditionally, international actors sought control over resources, actions, and certain events and outcomes.[17] However, Russia does not always seek physical control. Through an efficient use of IW, it spreads domestic chaos for its adversaries—a form of psychological control.[18] Misinformation and disinformation is a tool used by the Soviets, but Russia has frequently deployed them again, especially with the proliferation of the internet and social media—it is another sophisticated tool in its international relations toolbox.[19] The 2016 U.S. presidential elections and the chaos that followed exemplify this point.[20] The Russian IW strategy uses ICT platforms to undermine, manipulate, and mislead the information people consume as it believes this can advance its political and military objectives. Further, information warfare can disorganize governance and governments. It can "reeducate" certain groups and societies with a specifically designed curriculum that will yield Russia's desired outcomes in the future. It is also important to mention that in order to control global events, Russia does not rely solely on new media and social networks but also on more traditional media such as television and print media.[21]

Russian Cyber IW: Methods of Strategic International Distribution

The Russian IW in the Baltic, Scandinavian, and East-Central European states serves as a very significant and insightful lesson and helps explain how IW operations are designed and executed and how they are a continuation of Soviet active measures. As this article suggests, Russia's use of sharp power exposes the systematic asymmetry between its restricted cyber domain and the openly free cyber domain of its adversaries. To understand why Russia is spreading disinformation in the above-mentioned region, it is important to understand why the region is of strategic significance to Russia. The Baltic, Scandinavian, and East-Central European regions consist of Denmark, Sweden, Norway, Finland, Germany, Poland, Estonia, Lithuania, Latvia, and Russia. It is Russia's geopolitical backyard and some of its members are ex-Soviet states. Since 1994, Estonia, Latvia, and Lithuania joined the Partnership for Peace program and became North Atlantic Treaty Organization (NATO) members as well as European Union (EU) members in 2004. From that moment on, Russia sought more influence in the region in order to resist Western military and economic influence. NATO's growing power in the Baltic and Scandinavian region had effectively created a security dilemma for Russia—it had no choice but to resist.[22]

Most of the Baltic and Scandinavian states are NATO members apart from Sweden and Finland. Thus, learning from past mistakes, Russia chose to protect its backyard not with hard power, as the Soviet Union had once done, but with a smart use of IW power. In case Sweden and Finland were to join NATO, it could deter Russia from engaging in conflicts and seeking more influence in the region, as an attack on the alliance could trigger NATO's article 5, meaning that an attack on any ally is considered an attack on all allies. In such a scenario, Russia risks engaging in a conventional war with all NATO allies on its Western border and a potential direct conflict with the United States, if not worse.[23]

Moreover, as Richard D. Hooker Jr. argues, Russia has strengthened itself and its borders in Georgia (2008) and Ukraine (2014) with a calculated risk between annexation, international escalation, and Russia's least favorite option of letting Georgia or Ukraine get even closer to the West—indeed, after Russia's actions, the Georgian attempt to join NATO halted and the pro-European movement in Ukraine faded away to some extent.[24] The next point of conflict will probably be in the Baltic or Scandinavian region where, on the one hand, Russia will pressure NATO members to reduce their activities with the alliance, while, on the other hand, pressure nonmember states such as Sweden and Finland to reject alliance membership. Russia seeks to keep the status quo of isolating Estonia, Latvia, and Lithuania from the rest of NATO by sabotaging Western efforts to bring Sweden and Finland into NATO.[25] To keep Sweden and Finland away, Russia knows it must win their hearts and minds. Rather than creating a zero-sum game, Moscow attempts to win the information war—to persuade the Swedish and the Finnish citizens into pressuring their policy makers, via elections, out of any future NATO cooperation and agreement. Thus, a successful disinformation campaign can effectively undermine Western presence and NATO's power, or perception of power, by its members.[26] In fact, Russia's strategic concept is simple but effective; instead of resisting the West and NATO as an entire bloc, head-to-head, it uses the technique of divide et impera, spreading disinformation in each of its adversaries to divide them.

In January 2017, the Swedish Institute of International Affairs accused Russia of spreading disinformation and misinformation as part of a coordinated IW campaign to influence public opinion and decision making in Sweden. As Anders Thornberg, former head of Sweden's security service, the SÄPO, argued in January 2018, Russia tried to spread chaos in Swedish society before the September 2018 elections to prevent a unanimous decision of joining NATO.[27] In Finland, Russia had spread disinformation about the European migration problem to promote nationalism, xenophobia, Islamophobia, and divide the left and right political spectrums.[28] In another example, Russia promoted social media bots and trolls and created a smear campaign against Finnish journalists and researchers who educated the public about the Russian misinformation campaigns. Another more prominent example is the “Lisa case” in Germany. To spread xenophobia in Europe in general—Sweden and Finland in particular as well as in Germany—Russia backed a false news story claiming a German-Russian girl was raped by Arab migrants.[29] Further, Russia promoted misleading information to make the Finnish and the Swedes fear Westerners—not just migrants from other cultures. It has spread a false rumor that NATO soldiers could potentially rape Swedish women without fear of prosecution as they are immune from it due to their NATO service.[30] It had also spread a debate on whether NATO would stockpile nuclear weapons on Swedish and Finnish soil in secret places due to its proximity with Russia, if they should join NATO.[31]

In general, recent Russian IW tactics include disinformation and misinformation, use of bots and trolls in social media and in other websites, and the “authentication” of forged information by assigning them to allegedly legitimate news agencies that cover such stories. Russian state-sponsored news agencies include RT and Sputnik. Ahead of the 2020 election in the United States, Daniel Ray Coats, former director of U.S. national intelligence, highlighted the Russian cyber-IW threat:

> We assess that Russia poses a cyber espionage, influence and attack threat to the United States and our allies. Moscow continues to be a highly capable and effective adversary, integrating cyber espionage, attack and influence operations to achieve its political and military objectives. Moscow is now staging cyber-attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat—an issue discussed in the Online Influence Operations and Election Interference section of this report.[32]

Liberal democracies are worried since some cyber warfare tactics such as espionage, propaganda, and data manipulation are not illegal in the current state of affairs between states. Though each state has or can have laws and regulations, they cannot compel other states. There is no applicable law regarding cyber warfare. According to the 2017 revision of the *Tallinn Manual on the International Law Applicable to Cyber Operations*, which is only a proposal for cyber warfare for international laws, the previously mentioned cyber tactics are not illegal. That is, misinformation and disinformation and espionage for the purpose of misinformation and/or disinformation is legal. Moreover, cyber warfare attacks in general can be treated as kinetic attacks and retaliation can be justified only if the victim can prove who initiated the attack, with full forensic details.[33] This cyber forensic process is currently very problematic due to the use of privacy and anonymity tools as well as the use of proxy players. Further, punishment against cyber warfare is not practiced and deterrence is slow, blunt, and ineffective.[34] Russia and every international player for that matter can spread disinformation freely. Retaliation may come, but it would not be justified by international law and could further escalate the conflict into kinetic means. As Yochai Benkler, Robert Faris, and Hal Roberts argue, a fundamental technological change occurred with the rapid development of social media and other forms of communication in recent years that created echo chambers, which in turn reinforced people's internal biases, removed their indicia of trustworthiness and, in general, overwhelmed the world.[35]

Further, in February 2020, Federal Bureau of Investigation (FBI) Director Christopher A. Wray said that Russia was engaged in IW attempts to influence the 2020 presidential elections, as it did in 2016 as well. Russia relies on a covert social media campaign aimed at dividing American public opinion and sowing discord, just as it had made in the Baltic, Scandinavian, and East-Central European states. Russia promotes fictional personas, bots, trolls, social media postings, and disinformation. These attempts raise the question of how democracies should resist. Interestingly, Wray had no positive answer, stating that the First Amendment restricts authorities from monitoring disinformation.[36]

Interestingly, Moscow's bots and trolls can spread chaos without the fear of prosecution. Russia spreads chaos and disorder in the United States, in potential NATO members, and in the rest of Europe while risking no legal retaliation. It wins by undermining the democratic nature of its adversaries, spreading chaos in their societies. A probable measure for countering this is more regulation—but if the United States, Sweden, or Finland regulate online activities, they will also harm independent parties and voices—an essential part of democracy, as these efforts would risk mistaking legitimate narrative campaigns for Russian IW.[37]

Russian Domestic Control: Resisting Foreign Influence and Domestic Antigovernment Activists

Russian authorities perceive cyberspace not only as an opportunity to manage IW against the West but also as a major threat to Russian national security, stability, and regime legitimacy as the free flow of information in cyberspace could undermine the regime and promote the so-called "colour revolution"—a term used to describe nonviolent protests and uprisings in autocracies and former Soviet states.[38] To execute IW operations without the fear of becoming the victim of IW operations itself, Russian authorities have strived to secure and protect the Russian information domain from foreign influence. In the 2000s, Russian authorities established control (direct and indirect) over the major television channels and newspapers, while in the 2010s most of the established internet mass media (e.g., major online newspapers) have been effectively censored to limit criticism of the regime.[39] Still, social networks, online video platforms, secure messengers, and foreign-based internet mass media remain a great concern as Moscow has no control over information on these platforms. Cyberspace remains a domain only partly controlled by the authorities, enabling a relatively free flow of information. Therefore, to prevent possible Western efforts to destabilize Russia (as perceived by the Russian leadership) through IW in cyberspace, Moscow has taken the necessary precautions.[40]

Consequently, Russian authorities, through legislation and cyber regulation, strive to control Russian cyberspace to prevent or deter, as much as possible, the dissemination of information that may mar the positive representation of Vladimir Putin's regime, or any activity that may endanger the regime's stability.[41] Therefore, Russian authorities seek to take control over the content of the information circulating in Russian cyberspace. This is exemplified by our qualitative analysis—we use process tracing, legislation review, and analysis to exemplify and prove our findings and arguments.[42]

The authors analyzed actions and legislation taken by the Russian government since 2014 to gain more power and control over cyberspace. Since 2014 and the Russian intervention in Ukraine, the struggle between Russia and the West has intensified, specifically in the cyber domain. The authors have reviewed major official sources containing the previously mentioned legislation: the official internet portal of legal information of the Russian Federation, which contains all legislative acts and amendments accepted in Russia; official data considering legislative activities of the State Duma (the lower house of the Federal Assembly of the Russian Federation) provided by the Duma; and the official site of the president of Russia, which provides detailed information regarding the legislation approved by the president.[43] Furthermore, the authors reviewed legislation that has attracted significant attention by civil society, human rights organizations (Russian and international), and businesses, due to the potential of the laws to violate basic human rights. Finally, the authors reviewed operational expenses necessary for the legislation's implementation, which range from freedom of speech restrictions to data retention procedures. Eventually, the authors took into consideration only the most significant and prominent legislative acts and their amendments, which have had real (nonsymbolic) impacts on Russian society, and in fact have been implemented by the Russian authorities.

Generally, the most prominent Russian legislation directed at control over domestic cyberspace could be separated into the two major categories, which are also interconnected and represent one holistic perspective of information operations (offensive and defensive). This article defines these two categories as legal-technological and legal-psychological, which considers their impact on Russia's cyberspace and population and aligns with Russia's vision of offensive cyber operations. Also, in Russian IW campaigns, digital-technological and cognitive-psychological components are interconnected.[44]

Through appropriate regulation, Russia's authorities strive to establish control over Russia's cyberspace from the informational-technological perspective. At the same time, through the appropriate legislation, Russia's authorities strive to discourage its own population from undesirable activity in cyberspace (sharing information, writing undesirable posts, articles etc.), which from the authorities' perspective may endanger the stability of the regime—this is the psychological element.

The most prominent recent legal-technological efforts by Russian authorities consist of the following measures: the Yarovaya law; Russia's "sovereign internet" law; the mandatory installation of SORM (System of Operational-Investigatory Measures); and a law that makes Russian applications mandatory on smartphones, computers, etc.[45] This legislation (with the exception of SORM's mandatory installation, which for the first time was accepted in its current form in the 2000s) has been accepted in the last several years.[46] At the same time, the legal-psychological efforts consist of the three major measures: the "disrespect law" (18 March 2019); the "fake news" law (18 March 2019); and the new "foreign agent" law (2 December 2019).The Yarovaya law, passed in 2016, requires the provision of encryption/decryption keys on request by distributors of information such as internet and telecom companies, messengers, email services, forums, and other platforms that allow the exchange information to Russian special services such as the Federal Security Service (FSB). The encryption/decryption keys are necessary for decoding received, transmitted, delivered and/or processed electronic messages and information.[47] Moreover, according to this law, big data attributed to activity in Russian's cyberspace must be stored in Russian territory, while the special services should have unrestricted access to this data.[48] In practice, this law allows Russian special services to access private and corporate information circulating in the Russian segment of cyberspace. For example, companies like Facebook or Google must store information concerning data and activities of their Russian users in Russian territory and provide unrestricted access to the Russian special services. At the same time, the Yarovaya law is implemented only partially due to the technological difficulties and unwillingness to further aggravate the deteriorated relations with the Western countries and the Western technological companies.[49]

Furthermore, the Decree of the Government of the Russian Federation from 13 April 2005 (number 214) with changes from 13 October 2008 regarding SORM requires telecommunication operators to install equipment provided by the FSB. This allows the FSB and other security services to monitor unilaterally, without a warrant, users' communications metadata and content. This includes web browsing activity, emails, phone calls, messages, social media platforms, and so on. Moreover, the system has the capability of deep packet inspection—a filtering inspection point that filters transmitted data and weeds out noncompliant or unwanted material like spam, viruses or, in the context of this case, unwanted content and foreign websites. Thus, SORM is one of the major tools helping implement and regulate the Yarovaya law.[50]

Additionally, on 1 May 2019, President Putin signed and approved Russia's sovereign internet law, which allows the Russian internet to become independent and operate as an intranet, a stand-alone network outside of the World Wide Web. In practice, it allows Russia to operate an intranet, a restricted regional network such as what is used by large corporations or militaries. This network gives authorities the capacity to deny access to parts of the internet in Russia, potentially ranging from cutting access to particular internet service providers (ISPs) to cutting all internet access in Russia.[51]

Furthermore, on 2 December 2019, Russian president Putin signed a legislative bill requiring all computers, smartphones, and smart devices sold in Russia to be preinstalled with Russian software.[52] Later, the government announced a list of applications developed in Russia that would need to be installed on the above-mentioned categories of devices. This legislation was signed by President Putin on 8 December 2020, although its implementation and enforcement is delayed due to the COVID-19 global pandemic. In the near future, devices will be issued with government-issued serial numbers.[53] This will allow Moscow to tighten control over end users through regulation, monitoring, and surveillance. At the end of 2020, Russia's authorities continue preparations (including the legal and technological) for implementation of this legislation.

At the same time, the recent legal-psychological efforts consist of three major laws, as mentioned earlier, directed at prevention of distribution of facts and critiques directed at the government's activities and officials. For example, the law that regulates "disrespect" allows courts to fine and imprison people for online disrespect of the government, of Russian officials, of Russian human dignity, and public morality as the Russian Federation reserves the right to instruct citizens about proper public dignity and morality.[54] This law is very obscure—it allows the authorities the opportunity to interpret it as they wish. However, it is designed to prevent dissemination of information through informational-telecommunication networks only.[55]

An additional recent fake news law also outlaws the dissemination of what the government deems to be misinformative or misleading—any information undesirable by the government can be defined as "fake news."[56] Roskomnadzor (Federal Service for Supervision of Communications, Information Technology, and Mass Media), responsible for the Kremlin's censorship, is empowered by the law to notify the editorial body (or author) of the online publication that certain information must be removed from its website.[57] Moreover, the law prescribes heavy fines for knowingly spreading mis/disinformation and forces ISPs to deny access to websites disseminating it in the pretrial order following the appropriate decisions issued by the Roskomnadzor.[58]

The recent foreign agent law applies to any individual who distributes information on the internet and is funded by foreign sources. Interestingly, YouTube channels can be also defined as such.[59] According to this law, Russian citizens and foreigners can be defined as foreign agents. Consequently, all materials (including posts in social media) published by individuals who receive funds from non-Russian sources must be labeled as foreign agents.[60] A commission of the Ministry of Justice and the Ministry of Foreign Affairs have the power to recognize individuals as foreign agents. Therefore, foreign agents will be obliged to create a legal entity and tag messages with a special mark. Furthermore, individual foreign agents are subject to the same requirements as nonprofit organizations recognized as foreign agents (the law regarding nonprofit organizations was adopted in 2012). According to the law, foreign agents will be obliged to provide data on expenditures and audits regarding their activities to the Ministry of Justice.[61] It should be noted that these administrative obligations are time consuming, complicated, and expensive—they are aimed at discouraging so-called foreign agents from their activities. Apparently, this legislation is directed against antigovernment activists, vloggers, bloggers, independent journalists, independent politicians, and human-rights activists.[62] Overall, the purpose of the legal-psychological efforts is to discourage the population from participation in any kind of anti-government activities in cyberspace.

At the same time, the disrespect law, fake news law, and the new foreign agent law are implemented to discriminate against particular individuals, organizations, and sporadically in indiscriminate manner against the general population to intimidate people and discourage them from critiquing the regime.[63]

Therefore, it can be argued that Russian IW outside its borders is inextricably linked with the authorities' efforts to control Russian domestic cyberspace, and together they constitute one holistic framework of information security. This enables Russia to achieve tactical superiority over the openly pluralistic democratic West, as Russia can be considered a nondemocratic country with the previously mentioned legislation as well as other oppressive laws. Russia conducts IW against Western countries and organizations, while it limits the potential of possible Western IW operations in Russian cyberspace.

Conclusion: Russia Has the Upper Hand

The question examined in this article is how Russia employs information warfare on other players in the international arena but protects itself from IW. The authors' main argument is that while Russia executes influence operations and IW using cyberspace, it strives for uncompromising control over its domestic cyberspace. Russia restricts potential Western and undesirable domestic informational influence over its population. As discovered though the case studies of Russian intervention in the Scandinavian, Baltic, and East-Central European states, Moscow's bots and trolls affect Western democracies by effectively disrupting their democratic institutions. Russia undermines the democratic nature of its adversaries, dividing their societies between different ethnic groups and political persuasions, thus harming their governance. The targeted states are very limited in their responses as online regulation and moderation can potentially harm independent parties and voices, an essential part of democracy, as these efforts would risk mistaking legitimate narrative campaigns for Russian IW actions.

Many international players, including the West, use IW for their own advantage. However, in this case Russia has the upper hand. As discussed here, in the current state of affairs, Russia is winning in the cyber realm as it hits hard while blocking almost every major Western attempt of influence. Moscow influenced the United States, Britain, Europe, NATO, and many other countries and organizations, and it suffered only limited foreign interventions. Legislation such as the Yarovaya law or its sovereign internet law allows Russia to restrict the flow of undesirable information. For example, laws such as the foreign agent law discourage Russian citizens from regime criticism. Eventually, liberal democracies will need to strengthen their unique characteristics, revamp internet policies, and educate civilians in order to resist Russia's influence attempts. For democracy to prevail without the potential need to undermine their democratic nature, countries must enact efficient measures to contain hostile foreign propaganda.[64]

Endnotes

1. In this regard, China should also be mentioned as a unique case as it spreads information worldwide but vigorously restricts and protects its own cyber domain.
2. Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Foreign Affairs*, 16 November 2017.
3. Daria Litvinova, *Human Wrongs: How State-backed Media Helped the Kremlin Weaponise Social Conservatism*, Reuters Institute Fellowship Paper (Oxford, UK: University of Oxford, 2018).
4. Ronald Suny, *The Revenge of the Past: Nationalism, Revolution, and the Collapse of the Soviet Union* (Stanford, CA: Stanford University Press, 1993), 1–15.
5. Stephen G. Brooks and William C. Wohlforth, "Power, Globalization, and the End of the Cold War: Reevaluating a Landmark Case for Ideas," *International Security* 25, no. 3 (2001): 5–53.
6. Martin McCauley, *The Rise and Fall of the Soviet Union* (New York: Routledge, 2014), 437–52.
7. Ernest J. Wilson III, "Hard Power, Soft Power, Smart Power," *Annals of the American Academy of Political and Social Science* 616, no. 1 (March 2008): 110–24, https://doi

.org/10.1177/0002716207312618; and Joseph S. Nye Jr., "Get Smart: Combining Hard and Soft Power," *Foreign Affairs* 88, no. 4 (July/August 2009): 160–63.

8. Joseph S. Nye Jr., "Public Diplomacy and Soft Power," *Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 94–109, https://doi.org/10.1177/0002716207311699; and Patryk Babiracki, *Soviet Soft Power in Poland: Culture and the Making of Stalin's New Empire, 1943–1957* (Chapel Hill: University of North Carolina Press, 2015), 1–14.

9. An *influence operation* is the combined and synchronized application of diplomatic, informational, military, and economic abilities in times of peace or war that seek to influence decisions and behaviors or foreign targets. See Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica, CA: Rand, 2009), 3–6; and Bettina Renz, "Russia and 'Hybrid Warfare'," *Contemporary Politics* 22, no. 3 (2016): 283–300, https://doi.org/10.1080/13569775.2016.1201316.

10. Roger C. Molander, Andrew Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: Rand, 1996), https://doi.org/10.7249/MR661.

11. Timothy McCulloh and Richard Johnson, *Hybrid Warfare*, JSOU Report 13-4 (MacDill Air Force Base, FL: Joint Special Operations University, 2013).

12. Renz, "Russia and 'Hybrid Warfare'."

13. Nicholas J. Cull et al., *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It: An Analytic History, with Lessons for the Present* (London: London School of Economics and Political Science, 2017); and *Soviet Active Measures: Forgery, Disinformation, Political Operations*, Special Report No. 88 (Washington, DC: Bureau of Public Affairs, U.S. Department of State, 1981).

14. *GEC Special Report: Russia's Pillars of Disinformation and Propaganda* (Washington, DC: U.S. Department of State, 2020); and Richard Fletcher et al., *Measuring the Reach of "Fake News" and Online Disinformation in Europe* (Oxford, UK: Reuters Institute, University of Oxford, 2018).

15. Совет Федерации (Federation Council), "Концепция стратегии кибербезопасности Российской Федерации" (Concept of cybersecurity strategy of the Russian Federation) (n.d.).

16. Michael Connell and Sara Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: CNA, 2016).

17. Jeffrey Hart, "Three Approaches to the Measurement of Power in International Relations," *International Organization* 30, no. 2 (Spring 1976): 289–305, https://doi.org/10.1017/S0020818300018282.

18. Connell and Vogler, *Russia's Approach to Cyber Warfare*.

19. Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear?: How New Is Russia's 'New Way of War'?," *Small Wars and Insurgencies* 27, no. 2 (2016): 282–301, https://doi.org/10.1080/09592318.2015.1129170; and Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, 28 August 2016.

20. Matthew Chance, "Putin Has Relished US Political Chaos. He May Now Fear Trump's Impeachment," CNN, 12 November 2019.

21. Margarita Levin Jaitner and Kenneth Geers, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO CCDCOE Publications, 2015).

22. A. Thomas Lane, "The Baltic States, the Enlargement of NATO and Russia," *Journal of Baltic Studies* 28, no. 4 (1997): 295–308, https://doi.org/10.1080/01629779700000111; and Nivedita Das Kundu, "Russia's Baltic Security Dilemma," *India Quarterly: A Journal of International Affairs* 59, nos. 1–2 (2003): 59–72, https://doi.org/10.1177/097492840305900104.

23. John R. Deni, "The Paradox at the Heart of NATO's Return to Article 5," *RUSI Newsbrief* 39, no. 10 (November/December 2019).

24. Here, we argue that Russia had in fact strengthened itself with its actions in South

Ossetia, Abkhazia (Georgia, 2008), and Crimea (Ukraine, 2014). Though the Russo-Georgian war as well as the annexation of Crimea were costly in terms of economic, diplomatic, and military costs, Russia had successfully managed to push countries within its backyard away from the West, away from joining NATO, and away from further integration in Western and Central Europe. With far greater economic and military power than Georgia or Ukraine, the Russian calculated cost-benefit analysis turned to be a sound investment. See Wojciech Konończuk, "Russia's Real Aims in Crimea," Carnegie Endowment for International Peace, 13 March 2014; Kakhaber Kemoklidze and Natia Seskuria, "Twelve Years Since the August War, Georgia Still Faces Russian Aggression," *RUSI Commentary*, 12 August 2020; and Ariel Cohen, "The Russo-Georgian War's Lesson: Russia Will Strike Again," *New Atlanticist* (blog), Atlantic Council, 10 August 2018.

25. Richard D. Hooker Jr., "Operation Baltic Fortress, 2016: NATO Defends the Baltic States," *RUSI Journal* 160, no. 3 (2015): 26–36, https://doi.org/10.1080/03071847.2015.1054731; and Stephen J. Flanagan et al., *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance* (Santa Monica, CA: Rand, 2019), https://doi.org/10.7249/RR2779.
26. James Kirchick, "Russia's Plot against the West," *Politico*, 17 March 2017.
27. Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: Rand, 2018), https://doi.org/10.7249/RR2237.
28. Henri Mikael Koponen, "Finland Remains Resistant to 'Fake News,' Disinformation," International Press Institute, 24 January 2018; and Corneliu Bjola and Krysianna Papadakis, "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience," *Cambridge Review of International Affairs* 33, no. 5 (2020): 638–66, https://doi.org/10.1080/09557571.2019.1704221.
29. Stefan Meister, "The 'Lisa Case': Germany as a Target of Russian Disinformation," *NATO Review*, 25 July 2016.
30. MacFarquhar, "A Powerful Russian Weapon."
31. Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Washington, DC: Carnegie Endowment for International Peace, 2018).
32. Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019).
33. See Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, 2d ed. (Cambridge, UK: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.
34. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.
35. Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford, UK: Oxford University Press, 2018), 4, https://doi.org/10.1093/oso/9780190923624.001.0001.
36. Eric Tucker, "FBI Director Warns of Ongoing Russian 'Information Warfare'," AP News, 5 February 2020.
37. Michael Birnbaum, "Sweden Is Taking on Russian Meddling Ahead of Fall Elections. The White House Might Take Note," *Washington Post*, 22 February 2018.
38. Президент России (President of Russia), "Военная доктрина Российской Федерации" (The Military Doctrine of the Russian Federation), 5 February 2010; and "Секретарь Совбеза Патрушев призвал защитить молодых интернет-пользователей от зарубежных спецслужб" (Secretary of the Security Council of Russia Patrushev Urged to Protect Young Internet Users from Foreign Intelligence Services), *Newsru*, 19 July 2019.
39. Lilia Shevtsova, "Forward to the Past in Russia," *Journal of Democracy* 26, no. 2 (April 2015): 24, 29, https://doi.org/10.1353/jod.2015.0028.

40. Президент России (President of Russia), "Об утверждении Доктрины информационной безопасности Российской Федерации" (On Approving the Doctrine of Information Security of the Russian Federation), 5 December 2016.
41. Президент России (President of Russia), "Об утверждении Доктрины информационной безопасности Российской Федерации."
42. *Process tracing* is a qualitative methodology used to understand whether and how a cause or a set of causes have influenced a set of changes in a given case study.
43. Official portal of legal information, http://pravo.gov.ru/; State Duma (Federal Assembly of the Russian Federation), http://duma.gov.ru/en/; and the Kremlin (Presidential Executive Office), http://en.kremlin.ru/.
44. Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* 11, no 1 (Spring 2017).
45. Президент России (President of Russia), Федеральный закон от 06.07.2016 г. № 374-ФЗ (The Federal Law of 06.07.2019 No. 374-F3), 6 July 2016; "Joint Statement on Russia's 'Sovereign Internet Bill'," Human Rights Watch, 24 April 2019; Юлия Котова (Julia Kotova), "Госдума одобрила в основном чтении запрет на продажу смартфонов без российского софта" (The State Duma Approved a Ban on the Sale of Smartphones without Russian Software), *Forbes*, 19 November 2019; Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Ministry of Digital Development, Communications and Mass Media of the Russian Federation), Постановление Правительства РФ от 13 апреля 2005 г. N 214 (Decree of the Government of the Russian Federation of April 13, 2005 N 214), Об утверждении Правил организации и проведения работ по обязательному подтверждению соответствия средств связи (с изменениями от 13 октября 2008 г.) (On approval of the rules for organizing and carrying out work on the mandatory confirmation of the conformity of communication facilities, with changes from 13 October 2008); and Официальный интернет-портал Правовой информации (Official Internet Portal for Legal information), Федеральный закон от 02.12.2019 № 425-ФЗ (Federal Law of December 2, 2019 No. 425-F3), "О внесении изменения в статью 4 Закона Российской Федерации, О защите прав потребителей" (On amending article 4 of the law of the Russian Federation, about protection of consumer rights), 2 December 2019.
46. Nathalie Marechal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," *Media and Communication* 5, no. 1 (2017): 29–41, https://doi.org/10.17645/mac.v5i1.808.
47. Президент России (President of Russia), Федеральный закон от 06.07.2016 г. № 374-ФЗ (The Federal Law of 06.07.2019 No. 374-F3—Yarovaya Law), 6 July 2016.
48. Metadata is stored for a period of one year and data (messages of internet users, voice information, images, sounds, video, etc.) for a period of six months.
49. Юлия Степанова (Yuliya Stepanova), Юлия Тишина (Yuliya Tishina), "Операторам не грозит хранение в особо крупных размерах" (Operators are not in danger of oversized storage), *Коммерсантъ (Kommersant)*, 27 April 2020; and Анна Балашова (Anna Balashova), Мария Кокорева (Maria Kokoreva), Юлия Старостина (Yuliya Starostina), "Facebook и Twitter не получили отсрочку на перенос серверов в Россию (Facebook and Twitter have not received a grace period to move servers to Russia)," RBC, 1 October 2020.
50. Министерство цифрового развития (Ministry of Digital Development), Постановление Правительства РФ от 13 апреля 2005 г. N 214 (Decree of the Government of the Russian Federation of April 13, 2005 N 214).
51. "Joint Statement on Russia's 'Sovereign Internet Bill' "; and Вячеслав Половинко (Vyacheslav Polovinko), Юлия Минеева (Yulia Mineeva), Дарья Козлова (Daria Kozlova), "Желейный занавес: Власть усиливает давление на Сеть, но «сувернет» выходит из-под контроля даже своих создателей" (Jelly Curtain: The Authorities Increases Pressure on the Web, but "Sovereign Internet" Gets Out of Control Even of Its Creators), *Но́вая газе́та*, 8 November 2019.
52. Петр Харатьян (Petr Kharatyan), "Предустановку российского софта Госдума

одобрила без обсуждения с бизнесом" (The State Duma Approved the Preinstallation of Russian Software without Discussion with Business), *Ведомости*, 5 November 2019.

53. Совет Федерации, "Информация о законопроектах, внесенных в Государственную Думу сенаторами Российской Федерации в порядке реализации права законодательной инициативы" (работа завершена в 2020 году) (по данным СОЗД на 5 февраля 2021 года) (Information on bills submitted to the State Duma by senators of the Russian Federation in order to exercise the right to legislative initiative (work completed in 2020) (according to the data of the Social Development Fund of the Russian Federation as of February 5, 2021), 5 February 2021; Официальный интернет-портал правовой информации (Official Internet Portal for Legal information), Федеральный закон от 02.12.2019 № 425-ФЗ (Federal Law of December 2, 2019 No. 425-F3), 2 December 2019; Anton Zverev, "Putin Signs Law Making Russian Apps Mandatory on Smartphones, Computers," NASDAQ, 2 December 2019; and Дмитрий Шестоперов (Dmitry Shestoperov), "Рунет берут на карандаш: В какое целое складываются части регулирования цифровой среды" (Runet Has Been Taken Under Control), *Коммерса́нтъ*, 27 December 2019.

54. Официальный интернет-портал правовой информации (Official Internet Portal for Legal information), Федеральный закон от 18.03.2019 № 30-ФЗ (Federal Law of March 18, 2019 No. 30-F3).

55. Varvara Percova and Aleksey Sivashenkov, "Со всем уважением. Чем обернется для Рунета закон об оскорблении власти" (With All Due Respect. What Will the Law on Insulting Authorities Bring to Runet?), *Forbes*, 18 March 2019.

56. Президент России (President of Russia), "Подписан закон, устанавливающий административную ответственность за распространение заведомо недостоверной общественно значимой информации" (Has Been Signed a Law Establishing Administrative Responsibility for the Deliberate Dissemination of False Socially Significant Information), 18 March 2019. False information is regarded as unreliable socially significant information distributed under the guise of reliable information that creates a threat to the life and health of citizens, property, and the threat of mass disturbance of public order and public safety.

57. "Russia: Russian President Signs Anti-fake News Laws," Library of Congress, 11 April 2019.

58. "Putin Signs 'Fake News,' 'Internet Insults' Bills into Law," *Moscow Times*, 18 March 2019.

59. 'Путин подписал поправки к закону «О СМИ» (Putin Signed Amendments to the «Media Law»), *Коммерса́нтъ*, 2 December 2019/

60. The definition of the term *foreign agents* is of great social significance for Russian natives due to Russia's authoritarian past.

61. Официальный интернет-портал правовой информации (Official Internet Portal for Legal information), Федеральный закон от 02.12.2019 № 426-ФЗ (Federal Law of 02.12.2019 No. 426-F3), "О внесении изменений в Закон Российской Федерации О средствах массовой информации" и Федеральный закон "Об информации, информационных технологиях и о защите информации."

62. Александр Воронов (Alexander Voronov), "В иностранные агенты могут записать блогеров, студентов и туристов" (Bloggers, students and tourists can be defined as foreign agents), *Коммерса́нтъ*, 25 November 2019.

63. "Freedom of the Net 2020: Russia," Freedom House, accessed 26 March 2021.

64. Kristina Hook, "Hybrid Warfare Is Here to Stay. Now What?," Political Violence at a Glance, 12 December 2018.

Propagandized Adversary Populations in a War of Ideas

Donald M. Bishop

Abstract: Disinformation, the disruptive effects of social media, and the prospect of information warfare increasingly preoccupy national security thinkers. In the twentieth century, years of prewar and wartime propaganda by the Axis powers and the Soviet Union made the World Wars and the Cold War longer and more costly. In this century, China and North Korea represent two nations that have propagandized their populations for 70 years, hardening them against informational initiatives. What are the lessons? How should the United States assemble a strategy to counter propaganda's effects?

Keywords: propaganda, informational power, operations in the information environment, information operations, influence operations, public diplomacy, information warfare, political warfare, gray zone, hybrid war, war of ideas, indoctrination, active measures, social media, World War I, World War II, Cold War, China, Russia, North Korea

The national security community in the United States is now grappling with informational factors in great power competition, with cyber operations, network defense, defense forward, information warfare, political warfare, operations in the information environment, psychological operations, narratives, messages, influence operations, and the cognitive dimension in the

Donald M. Bishop is the Donald Bren Chair of Strategic Communications in the Brute Krulak Center for Innovation and Creativity at Marine Corps University, Quantico, VA. After serving in the U.S. Air Force in Vietnam, Korea, and on the faculty of the U.S. Air Force Academy, he was a public diplomacy officer in the Foreign Service for 31 years. He led U.S. public diplomacy in Bangladesh, Nigeria, China, and Afghanistan, and he was detailed to the Pentagon as the foreign policy advisor to the 34th Commandant of the Marine Corps, Gen James T. Conway. The author thanks John Thomson and Dr. William Morgan for their reviews of drafts.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201006

mix.[1] Different informational factors bear on all the traditional numbered operational phases and on the gray zone and hybrid war.[2] All hope that preparation and deterrence will prevent the outbreak of a shooting, kinetic, or hot war, but there would be informational dimensions to that kind of conflict too.

All this thinking can be sharpened by examining the wars of ideas in the twentieth century, with a particular focus on propaganda and its effects. During the two World Wars and the Cold War, the populations—and the armed forces—of several warring powers were highly propagandized. The internet, social media, and the cell phone have transformed the channels of propaganda, but in the twenty-first century, a few adversaries—China, North Korea, Russia, Iran, Cuba, and Venezuela—still draw on the experience of the twentieth century. They control the information that circulates in their societies, and they deploy domestic and international propaganda to strengthen their exercise of national power. What lessons of the past can help us see challenges of the present more clearly?

Contours of Propaganda

Propaganda has many definitions.[3] Many people consider ordinary advertising, with its characteristic puffery, as propaganda, along with social opinion campaigns—addressing the dangers of drugs, smoking, and alcohol—or environmental awareness, for instance.[4] The hype (exaggeration) and spin (biased interpretations) of political campaigns can be likewise criticized as propaganda.[5]

These forms of salesmanship and persuasion are, however, relatively benign. Communication surely becomes propaganda when falsehoods are included in a speech, argument, narrative, or appeal. These falsehoods include *disinformation*—lies—and/or the false attribution of sources.

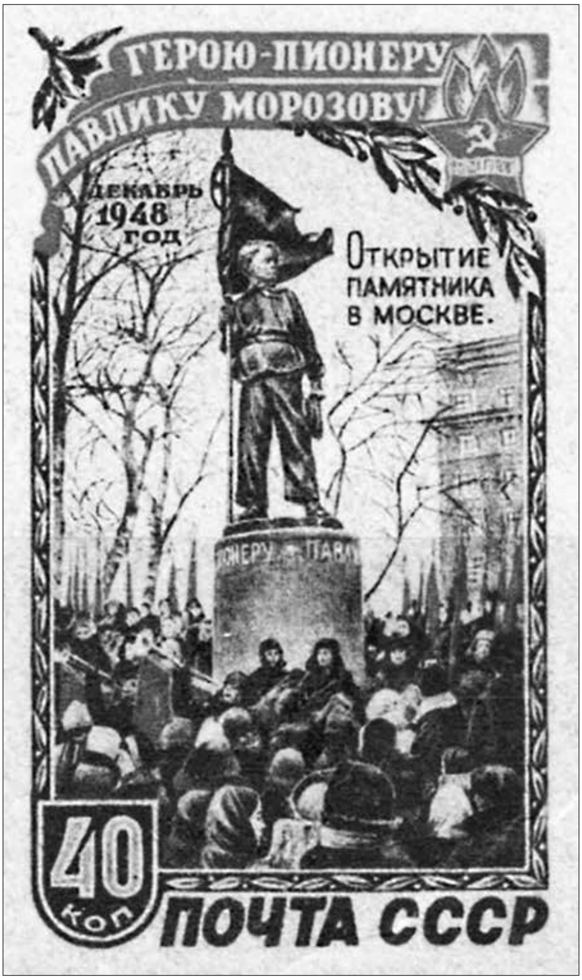
Psychology comes to bear. A small tumor of false information becomes more malignant when it is emotionalized.[6] There are many examples of propaganda inflating positive emotions like love, brotherhood, joy, or gratitude for a leader (fuehrer, duce, el caudillo, emperor, dear leader, father of nations) to develop a personality cult.[7] Propaganda can transform ordinary, positive patriotism into ultranationalism or hypernationalism. Propaganda can become even more dangerous when it stokes negative emotions like hate, envy, fear, disgust, anger, and even rage toward various "others."

The dictatorships of the last century, of course, used words to influence their populations, and they asserted control and direction of newspapers, magazines, books, and radio. When film and television became the dominant media, they melded control of words and images.[8] The regimes also used culture (dramas, dances, songs, and films) to propagate their views. The many posters circulated by the Soviet Union, the People's Republic of China (PRC), and North

Korea—still admired as art and studied as propaganda—show how art was used to express political and social messages.[9]

The dictatorships also took measures to insulate their populations from alternative views. State or ruling party officials reviewed articles, essays, and books before publication; only those that conformed to the regime's propaganda lines were published. Foreign publications were seized by customs inspectors at points of entry. International broadcasts were electronically jammed.[10] And arrests and disappearances of dissidents and nonconforming writers spread fear that served the regimes' censorship goals.

Figure 1. Commemorative stamp



In 1950, the Soviet Union issued a postage stamp to mark the unveiling of a statue of Pavel Morozov (1918–32). Morozov was praised as an exemplar for Soviet youth after he denounced his father to authorities; he became a Young Pioneer martyr when he was allegedly killed by "kulak" villagers. His grave became a shrine visited by generations of Soviet youth. The story was revealed as false after 1991 and serves as an example of a cult based on falsehoods, indoctrination of youth, use of publications, plays, music, and a postage stamp to spread a legend that served a dictatorship. (Scott #1445)

Source: Soviet Ministry of Communications, adapted by MCUP.

When the Bolsheviks, Nazis, or Chinese Communists took power, crushed independent media, spread their malign views, and purged independent thinkers, it was fear that cowed adults. They swallowed their own opinions before the brute force of the state. Year by year, however, the regimes—using schools, textbooks, and youth groups—increasingly made young people supporters of the regime and then obedient soldiers. In China's case in the 1960s, less than two decades after the establishment of the PRC in 1949, young Red Guards, animated by Chairman Mao Zedong and his *Little Red Book*, terrorized their own teachers and sometimes their parents.[11]

Two Propositions from the Twentieth Century

Although scholars may disagree on exact definitions and boundaries of propaganda, all agree that the warring powers of the twentieth century used propaganda, and the dictatorships, which could use coercion to suppress contrary opinions, developed it to the most extreme degree.[12] Two propositions—hypotheses—drawn from the wars of the last century may help us think through today's challenges.

Proposition 1: Both World Wars were longer and more brutal because of the prewar and wartime mobilization of combatant nation populations.

In the First World War, the growing human costs of the war justified Germany, France, the United Kingdom, and Russia's increasing use of propaganda on their populations to a degree that could not have been imagined before the war. Governments and high commands used speeches, rallies, print media, posters, music, newsreels, and film to promote their war aims, demonize their enemies, encourage recruitment, and increase production.[13] The combatant powers added domestic press controls and legal and police decrees to contain any sentiments or movements for peace. They prevented any discussion of military or diplomatic alternatives.

The history of the U.S. Committee on Public Information (CPI) led by "propaganda czar" George E. Creel during the First World War ("The Creel Committee") shows the United States was not immune from this wartime tendency.[14] However, American participation in the war lasted only 19 months, and two-thirds of all America's combat deaths occurred only in the final three months of the war, too short of a time for challenges about the conduct and costs of the war to gain traction.[15]

Examining propaganda in the Second World War, the late Czech historian Zbyněk Zeman made a salient point that "the fascist one-party states of the twentieth century and their leaders" along with "Lenin and the Bolsheviks all used political propaganda consistently and hard in peace-time as well as in war. The western liberal democracies, on the other hand, employed propaganda in war-time only."[16]

In World War II, Germany, Italy, the Soviets, and the Japanese went to war following years of psychological mobilization of their populations.[17] The particulars of the indoctrination were different in each of those totalitarian nations, but propaganda included idealizing certain racial groups—Aryans, or descendants of Yamato, for instance—while dehumanizing and persecuting disfavored minorities, the people of occupied areas, and the enemy as racially inferior, mongrels perhaps, or as class enemies.[18]

Those totalitarian states asserted full control over domestic newspapers, magazines, publishing, radio, drama, and film years before the war began. They sponsored and promoted approved art. They neutered the churches and the universities as independent incubators of ideas. They propagated their views to young people through the education system and youth groups. Again, these were not wartime measures; the regimes' messaging and narratives were developed long before war came, and they continued for years. After the fighting began, wartime censorship assured that domestic populations had no information that might weaken their allegiance to the regime or move them to question their support for the war.[19] Control of information and ideals was woven into the fabric of the warring regimes.

One result of the years of indoctrination was that soldiers and units continued fighting even when they took brutal casualties. Another was suicides among die-hard supporters of the regime. American Marines were horrified in 1944 to witness Japanese soldiers and civilians jumping to their deaths, many with members of their families, from "suicide cliff" on Saipan, and there were more suicides on Okinawa. These unfortunate women and men had been propagandized for many years about the purpose of life (to serve the emperor) and with manufactured stories of American brutality.[20]

Proposition 2: A major downside of propagandizing a nation's people is that leaders, step by step, become locked in by their propaganda.

Adolf Hitler, Benito Mussolini, Joseph Stalin, and Japanese militarists had conceived their twisted philosophies in the years following the First World War. When they came to power, they used the informational tools of the state and/or the ruling party to saturate the population with their worldviews.[21] They fired, purged, arrested, jailed, sent to camps, or killed those with independent or contrary views.

The supreme leaders surrounded themselves with true believers who had thoroughly absorbed the beliefs the regimes propagated, so the judgments of everyone in the top leadership circle were marred. Decisions in the armed forces, government, education, and the media were likewise warped by the ubiquitous propaganda. As the war turned against the Axis powers, Hitler, the emperor of Japan and his war cabinet, and Mussolini could not face the facts that might allow them to make rational decisions about termination of the war. The last few weeks in the Berlin bunker or in the palace in Tokyo provide case studies of how Germany and Japan's leaders were completely out of touch with 1945's political and military realities.[22] Their views of the countries in the alliances arrayed against them were often crude stereotypes. These provide case studies of Vaclev Havel's observation that a "regime is captive to its own lies."[23]

Another consequence of propagandizing is that even if leaders come to the realization it is necessary to contain or back down from hostilities, populations, once aroused, may not assent. Japanese historian Sadao Asada noted that even in the summer of 1945, "fanaticism was not restricted to the military; the men and women in the street were thoroughly indoctrinated. Women practiced how to face American tanks with bamboo spears."[24] Imperial Japanese Army officers who learned of the emperor's decision to surrender after the atomic bombings attempted a coup d'etat. They murdered two general officers and hoped to seize the palace and the emperor.[25]

Many of the impressionable teenagers drafted by Germany in the last year of the war gave their lives to the ideas of the thousand-year Reich utterly in vain. We may, moreover, attribute the deaths of American, Soviet, British, Canadian, French, and Polish soldiers and airmen in the face of the young German warriors' *Panzerfausts* and 88 mm antiaircraft and antitank artillery to propaganda. The sacrifices of the kamikaze pilots and Japan's soldiers on the islands were likewise wholly useless; American sailors and Marines were killed as much by the twisted propaganda that motivated the Japanese soldier and sailor as by bullets, artillery rounds, and mortars.

Fascism was defeated in 1945. The Soviet party-state—which provided assistance to China, North Korea, and Cuba; supported "national liberation" movements in the Third World; crushed the Hungarian revolution of 1956; and sent its own draftees into Afghanistan—continued to rely on domestic and international propaganda, but it collapsed and ended in 1991.

In the 1990s, then, many imagined that the benign exchange of goods, services, and ideas, along with democratic debate, would help create a new world free of conflicts of the kind that had been aggravated by Axis or Soviet propaganda and falsehood.[26]

Seventy Years of Propagandizing

If we look at international competition and conflict in the twenty-first century through an informational lens, however, there are disturbing parallels to the past. The use of social media is new, but the basic patterns of propaganda remain the same.

In our century, we see a renewed prominence of large, illiberal idea systems—Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, Bolivarismo, Juche, and Putinism among them. Many new forms of racial or religious nationalism and/or supremacy are also in circulation—often promoted by authoritarian leaders. As for "othering," in China there are worrying features. Han chauvinism lies beneath the surface in China, and Tibetans and Uyghurs are increasingly subject to propaganda and social controls.[27] North Korea propagates extreme views of racial purity.[28] In a complex world, such ideas simplify, providing a satisfying distinction between a good "us" and a bad "them," which provides for a motivating groupthink ideology.

States have many means—the media, social media, textbooks, youth leagues, and ruling parties—to support and project these ideas to their own populations. And many states export them. We can look at three.

Russia

Thinking through the ideas dimension of great power competition, it is revealing to know that Vladimir Putin's measures to strengthen Russian patriotism draw on selected achievements of the Soviet Union—especially the victory in 1945. His concepts of how the educational system and domestic propaganda foster patriotism draw on Soviet models.[29] Anne Applebaum speaks plainly of Putinism as an ideology, enforced "through legal pressure, public propaganda and, if necessary, carefully targeted violence."[30]

Russia's outward deployment of informational power has been well mapped. Its military doctrines describe "information-technical" and "information-psychological" methods, paralleling cyber and influence in American thinking.[31] They are integrated into Russian concepts of hybrid war and gray zone conflict. In Crimea and Ukraine, Russia deployed disinformation on such a scale that scholars labeled it the "firehose of falsehoods."[32]

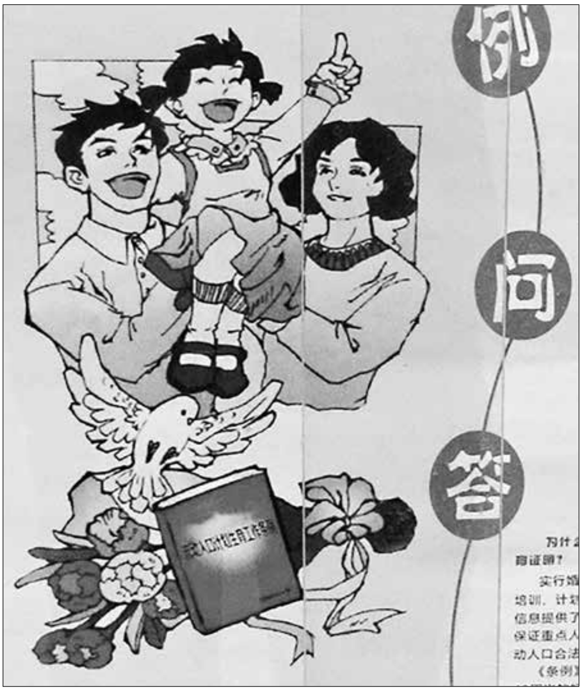
Russia has made substantial investments in two international broadcasting networks, RT (formerly Russia Today) and Sputnik.[33] The corporate mottos of the two networks—"tell the untold" and "question more"—flag their willingness to challenge journalism as it is practiced in Europe and the United States. Adroit use of social media, bots, trolls, inauthentic accounts, and deceptive websites were features of Russian disinformation during the 2016 U.S. presidential election.[34] They exploited America's domestic, internal divisions.[35]

China

China's people have now been subject to more than 70 years of propaganda and mobilization.[36] From the time of its origin in the 1920s, the Chinese Communist Party adopted Leninist concepts of propaganda. In his talks at the Yen'an Forum on Literature and Art in 1942, Chairman Mao Zedong stated that their purpose is to support class consciousness and the revolution.[37] The party's propaganda organs laid down approved and disapproved lines of thinking. After the Communists won the Chinese Civil War and established the People's Republic of China in 1949, they established dual state and party organizations to propagandize the Chinese people and the international community. In China today, there are media outlets owned by the Communist Party (e.g., *People's Daily*) and by the state (Xinhua News Agency), but the party also assures that privately owned media companies follow the party's lead. Removal of editors and shutdown of publications are among possible sanctions.[38]

China takes extensive measures to block international opinion. Newspapers

Figure 2. Domestic propaganda



Domestic propaganda—Shenzhen, China, 2009, promoting China's "planned fertility," meaning population control, policy. The title of the little red book is *Regulations to Implement Population and Planned Fertility Work*. The smiling faces gloss over the realities of sanctions, penalties, and forced abortions to lower population growth. As a result, China in the twenty-first century has a gender imbalance and too few working-age people to support a graying population. *Source: Courtesy of David and Jessie Cowhig, adapted by MCUP.*

may not directly quote foreign news sources; the government strictly limits the number of international correspondents in China and often calls them in for "interviews" if their reporting crosses a red line; and the Great Firewall prevents Chinese from accessing many foreign websites (e.g., Google, Facebook Twitter, Wikipedia, and the *New York Times*). A so-called 50-Cent Army monitors and manages social media.[39] In China, no one may see the 1989 photograph of "Tank Man" blocking the movement of PRC armored vehicles in Tiananmen Square.[40] Any circulation of the Tiananmen photograph or the facts about the origin of the Korean War will bring down the wrath of the regime. It is instructive that when People's Liberation Army (PLA) units were deployed to Beijing to clear Tiananmen Square of the students in 1989, the units were paused for last-minute indoctrination.[41] And even Winnie the Pooh is banned from China's domestic internet, due to the bear's use in memes and his alleged resemblance to Chairman Xi.[42]

China's outward projection of soft power includes the Belt and Road Initiative and the waves of Chinese messaging that support it, the Confucius Institutes in the United States, and the increasingly slick China Global Television Network.

As China becomes more prosperous, the size of its domestic box office has grown to nearly U.S. $2 billion, surpassing the North American box office for the first time.[43] In the past, Hollywood long hoped to capture more of the revenue by showing more American films in China's theaters, but Chinese authorities limit the number of foreign films that may circulate in the country, and foreign films must be submitted for review. As Joseph Goebbels barred the 1940 Hollywood film *The Mortal Storm* from showing in Germany, the PRC blocked such films as *Kundun*, *Seven Years in Tibet*, and *Red Corner* because they "viciously attack China [and] hurt Chinese people's feelings."[44] The 2016 remake of *Ben-Hur* only showed in China after "all references to Jesus were removed."[45] Hollywood gained more access through coproduction agreements, and many American stars have appeared in Chinese movies. Hollywood has, however, sold part of its soul to gain the additional revenue. Chinese censors assure that scripts do not in any way show China in an unfavorable light or contravene Communist Party propaganda lines. PEN America reported "the ways in which the Chinese government and its ruling Communist Party successfully influence Hollywood films" and stated that "this type of influence has increasingly become normalized in Hollywood."[46] China uses these arrangements to limit the exposure of its people to foreign values.

Speaking before a Senate subcommittee, the actor Richard Gere testified that

> there is no doubt that the combination of Chinese government censorship coupled with the desire of American studios to have access to China's market—soon to be the largest movie market in the world—and vast Chinese financing possibilities, can lead to self-censorship and to not engaging social issues that great American films and American studios once addressed.[47]

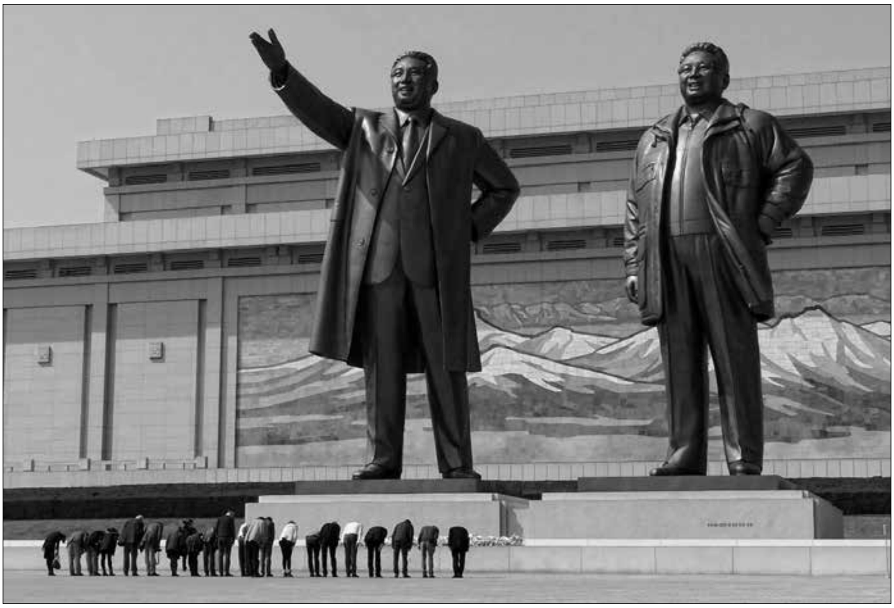
North Korea

Given Soviet and Chinese influence in North Korea since World War II, it is no surprise that North Korea also uses Leninist thought control and propaganda. The Korean Worker's Party (the public façade of rule by the Kim despots) announces and the state enforces what may or may not be expressed, and the party-state is not reluctant to jail those who dissent in its extensive network of prison camps.[48] A U.S. State Department report noted North Korea enforces three generations of punishment; "three generations of a prisoner's family are . . . sent to . . . camp[s] and may die there without having committed a crime themselves."[49]

The Kims' rule in North Korea is justified by a Paektu bloodline (descendants of Kim Il-Sung) and views of racial purity, and the North Korean party-state has ruthlessly demonized the United States for decades.[50] As in China, the North Korean party-state and its propaganda organs continue to assert that it was South Korea that attacked North Korea on 25 June 1950.[51]

North Korea follows the Chinese example of media and ideological control;

Figure 3. North Korean leadership



North Korea has a robust, all-encompassing system of domestic and international propaganda including a leadership cult; ultranationalist education; youth movements; indoctrination of its conscripts; full control of print, radio, and television broadcasting; radios and televisions pre-tuned to government broadcasts; limits on access to the internet; and museums that extol the revolution and the Kim dynasty and promote brutal caricatures of the United States.
Source: Courtesy of Bjørn Christian Tørrissen, adapted by MCUP.

the Committee to Protect Journalists, in its "10 Most Censored Countries" list, judges North Korea in second place (after Eritrea).[52] Only a few members of the party political elite have access to the global internet.

The use of propaganda in China, North Korea, and Russia has some specific national characteristics, but there are clear parallels between their uses of domestic and international propaganda.

Assembling a Strategy

If decisions of top leaders, military commanders, and civilians in propagandized states may be warped by their own nationalized, racialized, and propagandized belief systems, an effect of the propaganda could be the escalation of a dispute or conflict into phase 3. Units in the armed forces and the civilian population might offer stiff resistance due to their indoctrination. This suggests that national security community and armed forces commands need more focus on informational factors.[53]

These anxieties about propagandized adversary populations may seem distant from the many discrete cyber, information operations (IO), and electronic warfare (EW) issues that confront American businesses; civil society; local, state, and federal governments; and the armed forces. They do not directly address cyber defense, cyber offense, defense forward, or all the worrying developments of cyber, disinformation, misinformation, bots and trolls, inauthentic accounts, deepfakes, runaway memes, the proliferation of fake news, intrusion, meddling, and so on. But cyber and informational strategies must recognize how thoroughly the populations of major potential adversaries have been propagandized—and thus hardened against many informational initiatives contemplated by the United States and its allies and partners.

The new prominence and scale of informational challenges to U.S. national security suggest that needs are greater than the cyber expertise of Fort Meade in Maryland, more than the information operations prowess centered at Fort Bragg in North Carolina, more than competence of the "-39" staff sections at commands.[54] Surely whole-of-government and whole-of-society (Silicon Valley included) efforts are needed. The full scope of these needs and responses are larger than this article, but a focus on propaganda suggests these lines of effort.

Studies

The early section of this article offers two propositions derived from the World Wars. They invite scholarship. Question 1: Do modern states indeed have the same domestic propaganda powers? Question 2: What case studies support the propositions? For instance, what role did domestic propaganda play in shaping the actions of people ruled by Mussolini, Saddam Hussein, Muammar Gaddafi, the Argentine junta, Robert Mugabe, the Kim dynasty, Le Duan, and other dictators and autocrats? Think tanks and war colleges might offer insights based on history.

Systems of Control

Looking at the states that concern us, more knowledge of their systems of control is needed. Surely their command and cyber nodes and networks are a part of systems of control, but here the phrase means something larger. It also means knowing how these states and party-states develop approved lines of thinking and then propagate them. Before a North Korean student in a classroom reads—or a Russian listener hears—an approved narrative of history or international affairs or develops a hostility to the United States or another country, how has that narrative line been developed? What political, ideological, cultural, religious, racial, and historical threads have been woven together? What is the hostility quotient? How is the approved narrative spread over formal and informal networks? How do the carrots and sticks work? Awareness of systems of control in this larger meaning may be suggestive for defensive or offensive responses.

A Deeper Bench

Informational challenges require us to have more depth on the politics, history, languages, and cultures of nations of concern. If China is now the pacing threat, for instance, we need more Americans who read and speak the languages of China and have had firsthand experience in that society, enabling them to sense the cultural, informational, and psychological environments there.[55]

What is needed is not a new tent city at the Defense Language Institute in Monterey, California, for hundreds of students in uniform to learn the languages of China. According to John Thomson, former director of the Inter-University Program for Chinese Language Studies at Tsinghua University, more money for Chinese language programs in high schools and universities will likely have less impact than a targeted expansion of funding for Chinese (and Russian and Korean) language education in programs in those countries.[56] Different federal programs that support language study need to be aligned, and the government agencies that need China specialists should review their recruiting. Congress and the private sector should provide more money to support the China and Taiwan (and Russia and Korea) programs at U.S. policy institutes. Enlarging our nation's bank of expertise cannot be achieved even in a few years, so we need to begin yesterday.

Whole-of-Government Approach

If we speak of a war of ideas, even the amazing intellectual resources of the Department of Defense (military and civilian, direct hire and contractor) are insufficient. It is time to redouble whole-of-government initiatives. On the one hand, the Department of State must be a full partner—not just the new Global Engagement Center but also the larger Foreign Service and Civil Service, along with embassies and consulates.[57] Department of State personnel must join more wargames, exercises, and simulations. The Department of State's foreign policy advisors at military commands need to participate in the planning of operations in the information environment and join conversations on political warfare. Relations between State Department officers and the military information support teams sent by Special Operations Command to some embassies needs strengthening.

There is more to this whole-of-government imperative. The Coast Guard has specialized expertise. So do many other federal departments and agencies like the U.S. Treasury and Justice departments. The broadcasting networks under the U.S. Agency for Global Media—the Voice of America is the flagship—work within certain statutory boundaries and firewalls, but they must be part of a comprehensive response.[58]

A Clearinghouse

Since the Russian cyberattacks on Estonia in 2007, a growing number of policy institutes (first in Europe, then in the United States) have helpfully studied and analyzed Russian information operations.[59] Parallel but piecemeal efforts in the Pacific focus on Chinese and North Korean disinformation. Some of the think tanks publish regular disinformation exposés and alerts, but there is no agency or clearinghouse that rapidly disseminates their findings throughout the democracies. This is an unmet need.

Disabling Adversary Propaganda

Unraveling the propaganda that reaches millions of citizens of a state, shaping their worldviews and their hostility, is the work of years and decades, not weeks or months. Part of the effort is technical—how to reach those people when authoritarian regimes are determined to keep other views out. Broadcasting can reach some; virtual private networks (VPNs) can allow individuals access to the open internet; there may be cyber options to increase the penetration of alternatives to the views of a party-state.[60] But having the ability to broadcast into North Korea, for instance, would be only part of what is needed. The harder part is to think of what ideas to communicate.

American informational doctrines—for public affairs, for operations in the information environment, for broadcasting, and for public diplomacy—all agree that communication must be truthful.[61] Propaganda is not just repeated and shrill messaging; it always includes untruths. Identifying the lies embedded in propaganda is a starting point. Finding skillful and culturally appropriate ways to undermine and eventually discredit them is the next step. Any offensive in the realm of ideas must firmly anchor on truth.[62]

Declarative messaging of truth versus lies is often, however, too blunt. The creative sectors in the free societies—filmmakers, journalists, novelists, playwrights, artists, songwriters, performers, humorists—have ways to show truths that coax minds away from received ideas. This suggests that the showing of democratic culture has an important role to play.[63]

Shaping. Operations in the information environment conducted by military commands usually support specific operations, in specific geographic areas, during specific times. Facing populations that have been propagandized for many years, longer and broader efforts are needed, so a longer period of shaping must be part of any strategy. This long-term shaping may best be conducted by the State Department's public diplomacy and by the U.S. government's international broadcasting networks. Challenging propaganda and disinformation is already part of their missions, but comprehensive shaping calls for more collaboration with the informational elements of the Department of Defense.

Take encouragement from rivals' fears. During the Cold War, the Soviet Union spent billions to electronically jam broadcasts from the free world. Maintaining China's Great Firewall imposes large costs on its internet providers. The first demand recently made by Kim Jong-un's sister was that South Korean human rights groups cease sending balloons across the Demilitarized Zone (DMZ).[64] The small payloads of the balloons might include thumb drives with South Korean dramas and music, scriptures, and even Choco-Pies. These regimes know no society wants to be propagandized, nor do citizens want their lives bound by one party or autocratic leader.

Refreshing American values. During the World Wars and the Cold War, Americans faced rival ideologies with a relative consensus about national ideals. They included democracy, free and fair elections, separation of powers and federalism, the Four Freedoms, and an economy based on markets and enterprise.[65]

John R. Boyd, called by his biographer "the fighter pilot who changed the art of war," was the Air Force officer who conceived the energy-maneuverability theory and the OODA (observe–orient–decide–act) loop.[66] He prepared his famous "Patterns of Conflict" briefing during this period of relative consensus. His theories integrated the concept of a unifying vision "rooted in human nature so noble, so attractive that it not only attracts the uncommitted and magnifies the spirit and strength of its adherents, but also undermines the dedication and determination of any competitors or adversaries."[67]

In the current moment of social division in the United States, many Americans doubt the old American unifying vision, and our adversaries know it. That is why their own disinformation aims to stoke American division, undermine consensus, and erode democratic confidence. That is why our own efforts to counter their propaganda can be so easily countered by pointing out the distance between American ideals and social realities.[68] When Chinese Foreign Ministry spokesperson Hua Chunying was asked about American support for human rights in Hong Kong, she tweeted three words: "I can't breathe."[69]

This means that Americans who are focused on informational power must follow and join the conversations in our own society. Any new American narrative must now integrate the new findings of scholarship in history and many other disciplines that bear on the character of American society. Thinking through how to best present the United States must be part of a comprehensive informational strategy.

George Kennan, the architect of the containment strategy during the Cold War, concluded his famous "Long Telegram" of 22 February 1946 with these thoughts. In a time of worsening social division in the United States, they seem timely.

> Every courageous and incisive measure to solve internal problems of our own society, to improve self-confidence, discipline, morale and community spirit of our own people, is a

> diplomatic victory over Moscow worth a thousand diplomatic notes and joint communiqués. If we cannot abandon fatalism and indifference in face of deficiencies of our own society, Moscow will profit—Moscow cannot help profiting by them in its foreign policies.[70]

The Propaganda Factor

When policy makers and commanders think about confronting adversary nations, then, it is not enough to think about the military balance; weapons; land, naval and air power; and all the traditional topics. We must think about the propaganda that girds the power of these regimes and understand how their propagandizing affects both populations and members of the armed forces.

Totalitarian rulers still use propaganda and ideology as tools of control, and they still aim for dominance. They now add cyber and informational stratagems to project their brute ideas and power into other societies, including our own, and this adds an extra measure of risk in international relations and national security. The role of propaganda is one more factor to add when thinking about informational power.

Endnotes

1. "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." *Summary: Department of Defense Cyber Strategy, 2018* (Washington, DC: Department of Defense, 2018); "Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and postconflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives." Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica, CA: Rand, 2009), 2; *Information Operations*, Joint Publication (JP) 3-13, incorporating change 1 (Washington, DC: Joint Chiefs of Staff, 2014), said, "The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making."; *Information Operations*, I-2. See also Blagovest Tashev and Eric Gauldin, *Cognitive Dimension: A Culture General Framework* (Quantico, VA: Center for Advanced Operational Culture Learning, Marine Corps University, 2020), 1–3.
2. "Gray zone conflict is best understood as activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war. . . . They feature unconventional tactics, from cyberattacks, to propaganda and political warfare, to economic coercion and sabotage, to sponsorship of armed proxy fighters, to creeping military expansionism." Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, 5 February 2016. One thorough study is Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: Rand, 2018), 172–76, https://doi.org/10.7249/RR2942. The six phases are 0-shape, 1-deter, 2-seize initiative, 3-dominate, 4-stabilize, 5-enable civil authority. The phases are defined in *Joint Operations*, JP 3-0, incorporating change 1

(Washington, DC: Joint Chiefs of Staff, 2018), V-8–V-10. A large professional military debate challenging the construct is ongoing; see, for instance, Gen Joseph Dunford Jr.'s comments on Phase 2 1/2 at the Center for Strategic and International Studies, "Gen. Dunford's Remarks and Q&A at the Center for Strategic and International Studies," Joint Chiefs of Staff, 29 March 2016; and Gustav A. Otto, "The End of Operational Phases at Last," *InterAgency Journal* 8, no. 3 (2017). "Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies." "NATO's Response to Hybrid Threats," North Atlantic Treaty Organization, 16 March 2021. See also *MCDC: Understanding Hybrid Warfare* (Norfolk, VA: Multinational Capability Development Campaign, 2017); and Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Institute for the Study of War, 2015).

[3] Propaganda is the subject of an enormous literature. Short discussions include Bruce Lannes Smith, "Propaganda," Britannica, accessed 5 March 2021. "Propaganda, dissemination of information—facts, arguments, rumours, half-truths, or lies—to influence public opinion." See also "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News'," National Endowment for Democracy, 17 October 2017; and the excellent propagandacritic.com website.

[4] "Puffery Laws," Legal Match, accessed 17 March 2021.

[5] Issue 47 (2017) of *Foam: International Photography Magazine* forthrightly embraced and illustrated these broader definitions. The issue's theme was "Propaganda: No Power without Image Control," ed. Marloes Krijnen. See also Donald M. Bishop, "Photographers and 'Propaganda,' Friends and Enemies," Public Diplomacy Council, 26 March 2018.

[6] V Renée, "Watch: How Filmmakers Make Emotions Visual," No Film School, describes using "an overly dramatic song, shooting something in slow motion, or having an actor explicitly express an extreme emotion by crying, screaming, etc."

[7] A lengthy discussion of personality cults, with an extensive list of sources, comes from Anita Pisch, *The Personality Cult of Stalin in Soviet Posters, 1929–1953: Archetypes, Inventions and Fabrications* (Canberra: Australian National University Press, 2016), 50–54, http://doi.org/10.22459/PCSSP.12.2016.

[8] A retrospective on Soviet propaganda on the White Sea-Baltic Canal in 1933 shows the use of photographs in the service of narrative, illustrating the concept of "no power without image control"; and see David Campany, "USSR in Construction," *Foam International Photography Magazine*, no. 47 (2007): 91–110.

[9] Dozens of websites show Soviet, Chinese, and North Korean posters. One masterwork is Stefan R. Landsberger, Anchee Min, and Duo Duo, *Chinese Propaganda Posters* (Cologne, Germany: Taschen Bibliotheca Universalis, 2015). For the World Wars, Axis posters may be compared to British, French, Russian, and American posters, also found online. For thematic samples, see Zbynek Zeman, *Selling the War: Art and Propaganda in World War II* (New York: Exeter Books, 1982).

[10] Will Bohr, "Russian Jamming: The Electronic Iron Curtain," *Popular Electronics*, April 1959; and Rochelle B. Price, "Jamming and the Law of International Communications," *Michigan Journal of International Law* 5, no. 1 (1984): 400n6.

[11] Dramatic photographs of the period, hidden for many years, tell the story in Li Zhensheng, *Red-Color News Soldier* (New York: Phaidon Press, 2003).

[12] Zeman, *Selling the War*.

[13] Zeman's *Selling the War* helpfully outlined different themes of propaganda—patriotism, vigilance for spies and saboteurs, war production, "the international crusade," and the identification of foes as barbarians. Robert D. Leigh, the head of the U.S. Foreign Broadcast Intelligence Service during World War II, noted: "Around the world at this hour and every hour of the 24 there is a constant battle on the ether waves for the possession of man's thoughts, emotions, and attitudes—influencing his will to

fight, to stop fighting, to work hard, to stop working, to resist and sabotage, to doubt, to grumble, to stand fast in faith and loyalty." See Donald M. Bishop, "World War II and the Aims of Broadcasting," Public Diplomacy Council, 22 March 2019.

14. *Complete Report of the Committee on Public Information: 1917: 1918: 1919* (Washington, DC: Government Printing Office, 1920). George Creel, *How We Advertised America: The First Telling of the Amazing Story of the Committee on Public Information That Carried the Gospel of Americanism to Every Corner of the Globe* (New York: Harper & Brothers, 1920). The work of the Committee on Public Information (CPI) was effectively summarized by Nicholas J. Cull, *The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945–1989* (New York: Cambridge University Press, 2008), 6–9, https://doi.org/10.1017/CBO9780511817151. The most recent work is John Maxwell Hamilton, *Manipulating the Masses: Woodrow Wilson and the Birth of American Propaganda* (Baton Rouge: Louisiana State University Press, 2020). One CPI initiative was to organize thousands of "four-minute men" who would speak on the war during the four minutes that lapsed between the showing of each reel of a movie. For a pungent comment on the speakers, see Samuel Taylor Moore, *America and the World War* (New York: Greenberg Publishers, 1937), 76.

15. Michael Kazin, " 'War against War': Americans for Peace in World War I," *Constitution Daily* (blog), 6 April 2017. That "many Americans felt that criticism of the government was unpatriotic and even treasonous" provided one more reason for pressure against the campaign to gain votes for women; the incarceration of the "Silent Sentinels" is a chilling story; Ella Wagner, "Occoquan Workhouse," National Park Service, accessed 8 March 2021.

16. Zeman, *Selling the War*, 8.

17. Steven Luckert and Susan Bachrach, *State of Deception: The Power of Nazi Propaganda* (Washington, DC: United States Holocaust Memorial Museum, 2009) is a well-illustrated masterwork. Studies of propaganda in World War II usually only glance at the propaganda of Italian fascism, but "How Mussolini Won the Propaganda War: 1922–1943," Flashbak, accessed 8 March 2021, can open the door to the larger literature. Italian fascist art incorporated modernism in ways that German propaganda did not. In the foreword to a recent title on Soviet World War II propaganda, M. J. Trow opens boldly: "Twentieth century Russia was built on propaganda." *The Art of War*, vol. 3, *The Soviets* (London: BLKDOG Publishing, 2020).

18. A Beloit College historian notes, "The term has been used both as a kind of self-identification for in-group as well as a sometimes fierce expression of disdain for those who were not its members. This negative strain has been shown in Japanese perceptions of Koreans and Taiwanese during Japan's imperial period (1895–1945) and can be seen today with regard to treatment of Burakumin and other minority groups in Japan." See Robert Lafleur, "Asian Ethnicities (2a)—Japan ('Yamato')," *Round and Square* (blog), 11 July 2007. "Adolf Hitler had his own version of that view: Americans would never be able to defeat the Thousand-Year Reich, he assured his aides, because they were a mongrel people." Geoffrey C. Ward, "Mongrel Nation," *Smithsonian Magazine*, November 2001. See also Gerhard L. Weinberg, "Hitler's Image of the United States," *American Historical Review* 69, no. 4 (July 1964): 1010, https://doi.org/10.1086/ahr/69.4.1006.

19. For the step-by-step process by which the Japanese media printed "little more than propaganda about war, virtually all of it false," see Eric Johnston, "Truth Hurts: Censorship in the Media," *Japan Times*, 8 August 2015.

20. Derek Faraoi, "The Horrifying Suicides of Saipan," 13th Floor, 24 August 2016. A few were caught on film: "Japanese Women Jump Over a Cliff in Saipan, Mariana Islands during World War II. HD Stock Footage," YouTube, posted 9 May 2014, 1:13 min., from 0:41 in the clip. See, for instance, Ota Mashide et al., "Descent into Hell: The Battle of Okinawa," *Asia-Pacific Journal* 12, no. 48, no. 4 (November 2014). The mix of motivations among Japanese and Okinawans is still being explored by historians; see "Japanese Mass Suicides," Atomic Heritage Foundation, 28 July 2016; and Linda Sieg, "Historians Battle Over Okinawa WW2 Mass Suicides," Reuters, 6 April 2007.

21. Zeman, *Selling the War*, 12–28, discusses propaganda themes and organizations.
22. The best general accounts are John Toland, *The Last 100 Days* (New York: Random House, 1966), 451, 480; and Richard B. Frank, *Downfall: The End of the Imperial Japanese Empire* (New York: Random House, 1999), 288–330. The state of mind of Hitler and his ardent supporters in the *Fuhrerbunker* in Berlin in late April 1945 is well portrayed in *Der Untergang* [*Downfall*], the 2004 German film produced by Bernd Eichinger, 156 min. The film is based on Joachim Fest, *Der Untergang: Hitler und das Ende des Dritten Reiches* (Berlin: Alexander Fest Verlag, 2002); Joachim Fest, *Inside Hitler's Bunker: The Last Days of the Third Reich*, trans. Margot Dembo (New York: Farrar, Straus, and Giroux, 2004); Trudi Junge, *Bis zur letzten Stunde: Hitlers Sekretarin erzahit ihr Leben* (Munich: Claassen, 2002); and Trudi Junge, *Until the Final Hour: Hitler's Last Secretary*, trans. Anthea Bell (New York: Arcade Publishing, 2004).
23. It is worth reading the whole passage: "Because the regime is captive to its own lies, it must falsify everything. It falsifies the past. It falsifies the present, and it falsifies the future. It falsifies statistics. It pretends not to possess an omnipotent and unprincipled police apparatus. It pretends to respect human rights. It pretends to persecute no one. It pretends to fear nothing. It pretends to pretend nothing." Vaclev Havel, "The Power of the Powerless," *Amor Mundi*, 23 December 2011, originally published October 1978.
24. Sadao Asada, "The Shock of the Atomic Bomb and Japan's Decision to Surrender: A Reconsideration," *Pacific Historical Review* 67, no. 4 (November 1998): 511. This article does not directly examine the factor of a propagandized Japanese population but the effect of ultranationalism on the army leadership, especially, is more than implicit.
25. For a journalist's treatment of the "Kyujo Incident," see Ian W. Toll, "An Attempted Coup Tried to Stop Japan's Surrender in World War II. Here's How It Failed," *Time*, 11 August 2020.
26. A much-noted essay said "ideological violence" was to be replaced by "an unabashed victory of economic and political liberalism"; and Francis Fukuyama, "The End of History?," *National Interest*, Summer 1989, 1.
27. *Congressional-Executive Commission on China, 2020 Annual Report* (Washington, DC: Congressional-Executive Commission on China, 2020), 295–331; Kelsang Dolma, "Tibet Was China's First Laboratory of Repression," *Foreign Policy*, 31 August 2020; "China: Tibet Propaganda Masks Repression," Human Rights Watch, 19 June 2017; John Sudworth, "China's Pressure and Propaganda—The Reality of Reporting Xinjiang," BBC News, 15 January 2021; and Clarissa Sebag Montefiore, "How China Distorts Its Minorities through Propaganda," BBC, 15 December 2013.
28. B. R. Myers, "North Korea's Race Problem," *Foreign Policy*, 11 February 2010.
29. To know more about the indoctrination of Russian soldiers, see Ray C. Finch, USA (Ret), "Ensuring the Political Loyalty of the Russian Soldier," *Military Review*, July–August 2020, 52–67.
30. Anne Applebaum, *Putinism: The Ideology* (London: London School of Economics and Political Science, 2013). For the difficulties and contradictions of "patriotism," see Masha Lipman, "Putin's Patriotism Lessons," *New Yorker*, 24 September 2012.
31. Keir Giles and Anthony Seaboyer, *The Russian Information Warfare Construct* (Kingston, ON: Royal Military College of Canada, 2019), 9.
32. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model* (Santa Monica, CA: Rand, 2016), https://doi.org/10.7249/PE198.
33. Gordon Ramsay and Sam Robertshaw, *Weaponizing News: RT, Sputnik and Targeted Disinformation* (London: Centre for the Study of Media, Communication and Power, King's College London, 2019).
34. *Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election,* vol. 2, *Russia's Use of Social Media with Additional Views*, 116th Cong., 1st sess. (1 November 2020).
35. Donie O'Sullivan and Dylan Byers, "Exclusive: Fake Black Activist Accounts Linked to Russian Government," CNN Business, 28 September 2017.
36. For the use of propaganda and indoctrination in the early years of the PRC, see Frank-

lin W. Houn, *To Change a Nation: Propaganda and Indoctrination in Communist China* (Glencoe, IL: Free Press, 1961), esp. 1–9. A more recent study that examines both domestic and international Chinese propaganda is Kingsley Edney, *The Globalization of Chinese Propaganda: International Power and Domestic Political Cohesion* (New York: Palgrave Macmillan, 2014).

37. Donald M. Bishop, "Xi Jinping on Art and Culture," Public Diplomacy Council, 1 July 2019.

38. Jin Ding, "Telling Real News from Propaganda: A Reader's Guide to Chinese Media," Global Investigative Journalism Network, 12 May 2020; Tom Phillips, "Chinese Newspaper Editor Sacked for Critcising Beijing's 'War on Terror'," *Guardian*, 2 November 2015; and "Newspaper Suspended in China in Alleged Retaliation for Investigation of Beijing Storm Death Toll," IFEX, 9 August 2012.

39. Han Rongbin, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army'," *Journal of Current Chinese Affairs* 44, no. 2 (2015): 105–34, https://doi.org/10.1177/186810261504400205.

40. Kelsey Ables, "The Forbidden Images of the Chinese Internet," Artsy, 16 July 2019.

41. "[S]everal former soldiers said they were fed a confusing diet of indoctrination at their encampments on the outskirts of Beijing. They studied the speeches of Mr. Deng [Xiaoping] and were told that the demonstrations were the work of a subversive minority bent on toppling the Communist Party." Andrew Jacobs and Chris Buckley, "Tales of Army Discord Show Tiananmen Square in a New Light," *New York Times*, 2 June 2014.

42. Stephen McDonell, "Why China Censors Banned Winnie the Pooh," BBC News, 17 July 2017. The China Digital Times tracks "sensitive words"; see "Sensitive Word Series," China Digital Times, accessed 8 April 2021.

43. Patrick Brzeski, "It's Official: China Overtakes North America as World's Biggest Box Office in 2020," *Hollywood Reporter*, 18 October 2020.

44. Alexis Pogorelskin, "Phyllis Bottome's *The Mortal Storm*: Film and Controversy," *Space Between* 6, no. 1 (2010): 39–58; and Sharon Waxman, "China Bans Work with Film Studios," *Washington Post*, 1 November 1997. For *Red Corner*, starring Richard Gere, see "Can You Go Home Again?," *Newsweek*, 9 November 1997.

45. Martin Samoylov, "4 Hollywood Movies Banned by China," comingsoon.net, 24 August 2018.

46. *Made in Hollywood, Censored by Beijing: The U.S. Film Industry and Chinese Government Influence* (New York: PEN America, 2020). Compare the findings of this report with Benjamin Alexander Urwand, "Hitler and Hollywood: The Collaboration of American Movie Studios with Nazi Germany" (PhD diss., University of California, Berkeley, 2011).

47. Richard Gere, *Testimony before the Senate Finance Committee Subcommittee on International Trade, Customs, and Global Competitiveness*, 116th Cong. (30 June 2020). Other witnesses at the same hearing provided additional perspectives; see the testimonies of Beth Baltzan, Nigel Cory, and Clete R. Willems. See also "How China Is Taking Control of Hollywood," Heritage Foundation, 13 December 2018.

48. "Basic Facts about the Prison Camps," NK Hidden Gulag, accessed 9 March 2021.

49. "Prisons of North Korea," U.S. Department of State, 25 August 2017.

50. "North Korea Rewrites Rules to Legitimize Kim Family Succession," *South China Morning Post*, accessed 9 March 2021. See Preamble 10 of the "Ten Great Principles of the Establishment of the Unitary Ideology System," translation provided by the Citizens' Alliance for North Korean Human Rights, Bedford Row International, accessed 17 March 2021; Myers, "North Korea's Race Problem"; and "Lessons in Loathing at North Korea's Museum on 'US atrocities'," *Straits Times*, 7 June 2018. Art from the museum is prominent in the compilation of images by Gabe Paoletti, "21 North Korean Propaganda Depictions of Americans," allthatsinteresting.com, updated 8 June 2018.

51. For the mix of past and present propaganda in China and North Korea, see Tania Bran-

igan, "Korean War: 'There's Still the Evidence to Show It Was American Imperialism'," *Guardian*, 24 June 2010. North Korea's line is stated in Ho Jong Ho, Kang Sok Hui, and Pak Thae Ho, *The U.S. Imperialists Started the Korean War* (Pyongyang, North Korea: Foreign Languages Publishing House, 1993 reprint of 1977 edition).

52. "10 Most Censored Countries," Committee to Protect Journalists, 10 November 2019.

53. For a disturbing excursion into the dynamics that would follow a decision to use tactical nuclear weapons, see Col Thomas C. Greenwood, USMC (Ret), "Winning Battles Will Not Be Enough in a Great Power Conflict," *Marine Corps Gazette* 104, no. 11 (November 2020): 53–59. He noted, however, "China would likely hesitate to start a shooting war with the United States given that its adroit use of political, economic, and informational power (and coercion) has enabled it to achieve many of its policy goals at a fairly low cost."

54. In the general template of armed forces headquarters, the "3" (G-3 for the Army, A-3 for the Air Force, N-3 for the Navy, and J-3 for the Joint Staff and Combatant Commands) directs operations. Under the "3," the section responsible for information operations is the "39."

55. Peter Loftus, Jon Nesselhuf, and Howard Ward, "A War by Words: Language and Cultural Understanding in the Age of Information Warfare," *Journal of Indo-Pacific Affairs* (November 2020). For more views, see Ben Harburg, "Americans Don't Know China—and That's a Huge Problem," *Fortune*, 15 August 2018; and Chi Wang, "China 'Experts' and US-China Relations," *Diplomat*, 29 May 2018. The congressionally mandated assessment by the Center for a New American Security, *Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific* (Washington, DC: Center for a New American Security, 2020), included a number of proposals to increase language capabilities.

56. John Thomson, email to author, 2021.

57. "Global Engagement Center," Department of State, accessed 22 March 2021.

58. "Networks," U.S. Agency for Global Media, accessed 9 March 2021. The "Voice of America Charter" is in section 206 of Foreign Relations Authorization Act, Pub.L. No. 94-350. 22 CFR § 5313 codified a "firewall" to "protect" the "professional independence and integrity" of the VOA.

59. *Countering Russian Disinformation* (Washington, DC: Center for Strategic and International Studies, 2020). The work of the European External Action Service's East Stratcom Task Force is one of the best efforts; see "About," EUvsDisInfo, accessed 8 April 2021.

60. See, for instance, the website of Radio Free Asia's Open Technology Fund.

61. Policy documents that commit U.S. government organizations engaged in public affairs, public diplomacy, international broadcasting, and operations in the information environment to truthful and accurate communication are too numerous to list. The former under secretary of state for public diplomacy and public affairs, D. Bruce Wharton, addressed truth decay in his section, "Public Diplomacy in an Era of Truth Decay," *2018 Comprehensive Annual Report on Public Diplomacy & International Broadcasting* (Washington, DC: United States Advisory Commission on Public Diplomacy, 2019), 25–29.

62. Havel, "The Power of the Powerless"; Alexander Solzhenitsyn, "Live Not by Lies," *Index on Censorship*, no. 2 (2004): 203–7; and John Paul II, *Veritatis Splendor* [The splendor of truth] (Vatican City: Vatican, 1993).

63. For how the Propaganda Department of the Chinese Communist Party smothers creativity—less by censorship than by inducing self-censorship—see Ha Jin, "The Censor in the Mirror," *American Scholar*, 1 September 2008. Thus, "most Chinese movies lack depth and complexity—they're hamstrung at the outset by directors and producers having to worry about whether the final product will pass the censors."

64. "South Korean Balloons: Plans to Stop People Sending Cross-Border Messages," BBC News, 4 June 2020.

65. The "Four Freedoms" mentioned in President Franklin D. Roosevelt's State of the Union Address in 1941 were freedom of speech, freedom from want, freedom from fear, and freedom to worship. They became shorthand for the aims of the democracies in the Second World War. See Stephanie Haboush Plunkett and James J. Kimble, *Enduring Ideals: Rockwell, Roosevelt and the Four Freedoms* (New York: Abbeville Press, 2018); and Donald M. Bishop, "Revisiting the Four Freedoms," *Foundation: Marine Corps University Foundation Magazine*, Summer 2019, 3–7.
66. Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Boston, MA: Little, Brown, 2002). See also Ian T. Brown, *A New Conception of War: John Boyd, the U.S. Marines, and Maneuver Warfare* (Quantico, VA: Marine Corps University Press, 2018).
67. Chet Richards and Chuck Spinney, eds., "Patterns of Conflict, John R. Boyd" (presentation, Defense and the National Interest, January 2007), slides 143–44.
68. Faiza Patel and Raya Koreh, "New Method, Same Strategy: Russia Has Long Exploited U.S. Racial Divisions," Brennan Center for Justice, 23 October 2018. In his civil rights address on 11 June 1963, President John F. Kennedy obliquely acknowledged the power of this challenge when he said, "We preach freedom around the world, and we mean it, and we cherish our freedom here at home, but are we to say to the world, and much more importantly, to each other that this is the land of the free except for the Negroes; that we have no second-class citizens except Negroes; that we have no class or caste system, no ghettoes, no master race except with respect to Negroes?" See John F. Kennedy, "Civil Rights Address" (speech, White House, Washington, DC, 11 June 1963).
69. Adela Suliman, Ed Flanagan, and Justin Solomon, "China Jeers as George Floyd Protests Sweep U.S.," NBC News, 1 June 2020.
70. "George Kennan's 'Long Telegram'," 22 February 1946, History and Public Policy Program Digital Archive, National Archives and Records Administration, Department of State Records, Record Group 59, Central Decimal File, 1945–49, 861.00/2-2246; reprinted in U.S. Department of State, ed., *Foreign Relations of the United States, 1946*, vol. VI, *Eastern Europe; The Soviet Union* (Washington, DC: Government Printing Office, 1969), 696–709.

Social Antiaccess/Area-Denial (Social A2/AD)

Colonel Phil Zeman, USMC

Abstract: Social antiaccess/area-denial (A2/AD) describes the threat posed to U.S. and Western security by sociopolitical and socioeconomic means, primarily by China and Russia. This concern focuses on actions by China and Russia designed to fracture American and Western societies through information, disinformation, economic coercion, and creating economic dependencies—in many cases capitalizing on target nation propensities to accomplish strategic ends. Through these ways, China and Russia hope to prevent the will or ability of American or Western states to respond to aggressive acts.

Keywords: national security, antiaccess/area-denial, A2/AD, China, Russia

In the wake of the 1991 Gulf War, America's would-be adversaries took note of the overwhelming power of the U.S. war machine. They recognized the value and impact of our operational reach, technological overmatch (specifically precision targeting), martial proficiency, command and control, and doctrine. Acknowledging U.S. prowess in these areas, they devised strategies and techniques designed not to compete with the United States head-on, but to find weaknesses and opportunities to counter—and avoid—American military strength. To a significant extent, these developments have manifested themselves as antiaccess/area-denial (A2/AD) capabilities, designed to restrict American operational reach—most notably in antiship and antiair systems.[1] Just 10 years after Operation Desert Storm, U.S. and allied forces were again in action. The conflict in Afghanistan, shortly followed by entry into Iraq, was of a different character from Desert Storm, where American firepower and technological

Col Phil Zeman has served in the U.S. Marine Corps for more than 27 years in infantry, reconnaissance, strategy, and planning posts.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201007

prowess was not decisive—they proved only modest enablers. In searching for a viable response to this change in character, U.S. forces introduced the concept of war among the people, stipulating a shift in the conduct of military campaigns.[2] U.S. and allied forces focused campaign objectives on winning the support of the population and not purely the physical elimination of insurgents and terrorists. This population-centric approach appreciated the decisive roles of information, perception, and culture. This revised doctrinal approach recognized that populations—and with them, societies—are the basis of strength and power.[3]

The 2017 *National Security Strategy* returned the U.S. military to consideration of great power conflict.[4] Visions of the never-experienced great tank battles in Germany's Fulda Gap were now fused with twenty-first century weapons and technology.[5] This twenty-first century-remix of great power conflict is more than an update to previous conventional doctrine, as America's adversaries (both nation-state and nonstate) incorporate their observations from 1991, while adding a population-centric focus. This synthesis points to a different battlefield where the immense capability of the U.S. military is greatly reduced—or nullified altogether. While much discussion surrounds Chinese and Russian A2/AD networks and capabilities, the nonmilitary threat to the United States (and the West in general) receives muted attention—even in the face of repeated Chinese and Russian (among others) information and cyberattacks.

This emergent threat is subtle and coercive in nature, targeting not only the military or government but also industry and citizens. It is designed to exploit social dynamics and economic propensities by creating dependencies on foreign capacities. This strategic design is multifaceted; it exploits and expands the seams in democratic politics, degrades societal cohesion, and puts average citizens at risk while using those same citizens to create and expand economic dependencies—unwitting self-perpetuation of their own demise. Further, these actions are conducted simultaneously and comprehensively in a myriad of venues and ways, compounding the effect. This effort is opaque by design, with layers of complexity that inhibit identification and attribution. Indeed, even in the cases where nefarious actions are realized, other mechanisms deny and further obfuscate the actions while applying coercive countermeasures. Potentially the most significant element of this strategic approach is to never provide a casus belli sufficient to mobilize popular sentiment for response. The intent is not to defeat the United States or the West on the battlefield. The goal is to prevent the Unites States and its allies from even arriving on the field of battle by compromising national the socio-political-economic fabric to the point where it is unable, or *unwilling*, to respond to aggression. With voluminous discussion dedicated to penetrating and countering Chinese and Russian physical A2/AD networks, there needs to be a similar conversation surrounding the comprehensive nonmilitary targeting of America, with the intent to compromise American resolve, capability, and capacity to respond. America and the West need to recognize the threat posed by *social A2/AD*.[6]

Social A2/AD's main effort is to target the civilian population. It achieves this through information/disinformation campaigns as exhibited through its "Three Warfares" approach of public opinion warfare, influence warfare, and legal warfare, creating economic dependency through enticing corporate investment into Chinese markets, and fostering debilitating sociopolitical activity.[7] Notably, all of these disparate operations are interwoven, capitalizing on opportunities (often unwittingly created by the target population), while creating others. Further, it is important to recognize that there are multitudes of mechanisms that can be used to discreetly influence the social, political, and economic activity. Correspondingly, these domains continuously influence each other, compounding effects. As these dynamic influences interact, they also affect other elements, such as military power. Thus, the endgame of social A2/AD is to gain influence within a second or third state sufficient to prevent or restrict action against the instigating (aggressor) state.

Considering that social A2/AD is primarily a nonmilitary challenge, the well-trod dictums of the war theorist Sun Tzu provide valuable insights for defeating an opponent without force of arms: "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[8] Sun Tzu continues this line of thinking, stating, "Therefore I say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril'."[9] (Considering Sun Tzu was Chinese, it should be of little surprise that China would implement this approach. This is analogous to the discovery of gambling in a casino.) Further, a cursory understanding of the Chinese concept of *Shih* reinforces a people-centric view of strategy: "Since men and their hearts were critical to Shih-strategy, commanders and rulers needed to understand how to mobilize them."[10] Although Shih is typically in reference to one's own population and internal strength, it can simply be extended in reverse to an adversary; degrading the strength of your opponent's population is to your advantage. Using Sun Tzu's statements and Shih as a baseline, one can design a strategy designed to maximize indirect approaches and achieve victory without open conflict. This readily blends with the West's best-known military theorist, Carl Von Clausewitz, and his concept of center of gravity, by targeting your opponent's center of gravity while protecting your own.[11] Clausewitz explains that "one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends."[12] Simple analysis and synthesis of these principles provides a strong argument, and they become especially compelling when woven into a competitive, dynamic, strategy.

Elements of Social A2/AD

During the past decade, many of the attacks against the United States and other Western nations targeted populations, not governments. The Russian cyberattack on Estonia, interference in the 2016 U.S. presidential election, and Chinese hacking of the Office of Personnel Management (OPM) and Marriott hotels are a small sampling of such attacks and demonstrate the intent to disrupt and gain influence over civilian populations. Consider the potential effects, implications, and disruption caused by digital attacks targeting the individual finances of Americans (as "shaping" actions prior to a military campaign, or even as the chosen mechanism to alter behavior). What if these attacks came as the culmination of a comprehensive information campaign designed to convince a population that the so-called threat presented by Russia or China was nothing more than the fantastic conjuring of conspiracy theorists? Part of the campaign would include creating an environment hostile to development of preconflict safeguards and protections complete with twenty-first century "useful idiots" to champion China or Russia as misunderstood and wrongly accused. This information campaign would also find mechanisms to pit American versus American and ally against ally. China and Russia are not simply looking to compromise government systems and capabilities; they desire to hold private citizens and corporations at risk to degrade or prevent effective response, regardless of the mechanism, through societal friction, while discrediting and delegitimizing national leadership.[13]

Although American sociopolitical friction has become increasingly common (although few recognize the associated vulnerability), Europe may be even more susceptible to malicious information campaigns. With existing ethnic tensions, rising authoritarianism, and economic challenges (Brexit), increasing inter- and intra-European conflict appears an easy task. A European scenario requires little imagination: digital and information attacks culminate just as Russian forces conducting "exercise" Zapad in western Russia turn toward the Baltic states. As Russian brigades speed through Vilnius, Lithuania, to Kaliningrad, Russia, and occupy Riga, Latvia, and Tallinn, Estonia, something else takes place. The people of Germany, already with a pacifistic outlook, become enraged and disenchanted by information designed to simultaneously discredit national leadership, legitimize Russian actions (propaganda), and fracture social bonds. This leads to calls for immediate peace, with a simultaneous prohibition of North Atlantic Treaty Organization (NATO) forces transiting through Germany to the Baltics. Lacking access through Germany, the NATO response to Russian aggression in the Baltics is stopped cold. Although this scenario may seem fantastic, a 2015 Pew Research poll (done in the wake of the Russian intervention in Ukraine) found that German popular support for using force to support an ally from Russian military aggression was only 38 percent. Italy polled at 40 percent. Immediately threatened Poland fell in at 48 percent, and America's special ally, the United Kingdom, came in at 49 percent. The only countries to top 50 percent were the United States (56 percent) and Canada (53 percent).[14] The results of this poll indicate that NATO may face as much threat from within as from without. A Russian act that would trigger NATO's article 5, the collective defense article, could fracture the alliance between the nations that would and would not uphold treaty obligations.

The Pew Research findings are not harbingers of the demise of NATO; however, they do indicate opportunity for Russia (or China) to influence Europe. Russia has repeatedly used its dominant position in Europe's natural gas supply as a weapon of coercion.[15] China has lately also inserted itself into Europe's economic affairs:

> In 2016 Chinese investment in the European Union jumped to nearly €36bn ($40bn), up from €20bn the previous year, according to Rhodium Group, an American research firm. The recent purchases of major interest of major European ports such as Antwerp, Rotterdam, and Hamburg, or outright ownership of major ports (Piraeus) illustrate this point. Much of this is state-backed and speaks of the Communist Party's ambitions to keep Europe from helping America to contain China's rise.[16]

Further, through China's Belt and Road Initiative (BRI), the purchase and development of international transportation infrastructure has given rise to concerns about predatory loan practices—with indirect intended results that span physical, financial, and digital spectrums. By dictating the terms and conditions of predatory loans with associated project bidding requirements (prescribed use of Chinese construction and telecom companies), and bribing local officials, China has been able to gain advantage in countries across Asia, Africa, and even Europe. In some cases, China has turned this leverage into forced accommodation on items not previously envisioned. A prime example of this is China's leveraging of unsustainable loans to Sri Lanka into a Chinese People's Liberation Army Navy (PLAN) facility in Hambantota, Sri Lanka.[17] Sri Lanka is not alone in falling victim to predatory loans from China; many countries in the region are seen as debt risks due to Chinese BRI loans.[18] Punctuating the concerns is the extension of China's advanced digital structure, extending the "Digital Silk Road" across Asia—and with it, China's advanced surveillance apparatus.[19]

While China's financial practices have produced physical access abroad for the Chinese military, perhaps the most concerning element of access pertains to information and China's advanced surveillance apparatus. With China's Huawei at the forefront of 5G technology in Europe, the issue of information security has put the United States at loggerheads with two key allies, the United Kingdom and Germany, putting security-sharing agreements at risk.[20] Should Europe be enticed by Huawei's cheap 5G technology, it will serve as another layer of dependency on Chinese goods. Aside from concerns about Chinese surveillance, cost of future extraction would increase—both in terms of financial cost and China's ability to exert coercive power (not unlike Russia's ability to use natural gas as a lever in international discourse)—while simultaneously driving a wedge between long-standing, like-minded Atlantic allies. Although national security concerns are paramount, Chinese surveillance intrusion also presents a grave threat to Western values regarding the individual rights to privacy and information control and access. This, in turn, relates back to the targeting and holding at risk of citizens and private business—attacking the very fabric of Western society.

The above examples illustrate the immense potential of social A2/AD. Free-speech democracies are particularly vulnerable to these types of actions, as they take advantage of civil liberties held sacred by the United States and other open, free societies. In the European example, the Russians used social A2/AD to defeat a key military strength of the United States—its operational reach. That the Russians may or may not lack capability or capacity to fight the U.S. military in a multi-month campaign is irrelevant if the United States and its NATO allies are unable to get forces to the battlefield. Even if the United States and NATO were to find a path around the German impediment described above, Vladimir Putin would have already succeeded in gaining one of his most sought-after strategic objectives: gutting NATO through German rejection of an obvious article 5 event. If Russia or China successfully influence the *populations* of the champions of the existing global system, the impacts would be grievous for the existing world order and its leader, the United States. Defending democratic societies against authoritarian threats who would deceive, obfuscate, coerce, and subvert them must be the United States' and its allies' highest priority. Significantly, these concerns are just as real at home in the United States.

The special counsel investigation into alleged collusion with Russia presents an interesting example of the potential of social A2/AD. Acknowledging significant popular and media animosity toward President Donald J. Trump, it is easy to envision that the trickle of collusion-associated information was part of a scheme to drive further division within an already fractured U.S. society.[21] The point is not that the investigation itself is a Russian act, but that it provides an opportunity to exacerbate sociopolitical friction by providing information designed to push the investigation along, widening existing fractures within American society. Although it is impossible to prove a negative, it takes little imagination to see that Russia may have hedged its bets during the 2016 presidential election. Consider the ire of the Republican Party with the findings of the Federal Bureau of Investigation (FBI) probe into the Hillary Rodham Clinton email scandal, among other issues. These issues provide the ideal opportunity for disinformation coming from opaque sources to fan a flame of anti-Clinton sentiment designed to hamstring government action and increase existing societal friction. In either of these examples, emotion overtakes fact, propagated by a 24-hour news cycle and a social media environment dominated by the dramatic at the expense of truth. In *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, authors Peter Pomerantsev and Michael Weiss explain, "The Kremlin exploits the idea of freedom of information to inject disinformation into society. The effect is not to persuade (as in classic public diplomacy) or earn credibility but to sow confusion via conspiracy theories and proliferate falsehoods."[22] Even if both the above scenarios are off base, it is a common refrain that the current U.S. social environment is highly divided and antagonistic; U.S. society is ripe and open for exploitation. Sadly, much of this damage is done at the behest of China and Russia unwittingly; blinded by animosity, Americans are frequently the chief propagators of this intra-American social fratricide, serving Russian and Chinese interests as cyber and information goons. This concept is captured well by Douglass Rushkoff as he reintroduces the Leninist term of *useful idiots* for modern-day Russia:

> [L]ess important for their indictment of Trump and the agents he hired than for how they expose the way we all continue to buy into this manufactured animosity. So, no, the liberal elite did not infuse the landscape with today's more belligerent forms of identity politics. Neither did the far right invent the most contagious conspiracy theories about Hillary Clinton or George Soros. They are the result of four decades and hundreds of millions of dollars of targeted disinformation by Russia. Even more damaging than the stories themselves is how they make us feel about the "other side," who we believe has stooped to this level of shameful lying and rhetoric.[23]

The opioid epidemic, a front-page story within the United States, provides an even more sinister example of the breadth and cross discipline character of social A2/AD. As this crisis has grown in intensity, a new dynamic has emerged: China is a leading producer of both opioids and opioid precursor chemicals in what many call the "Reverse Opium War."[24] Further, much of the processing and transportation of these illegal drugs is done by Mexican cartels. Although widespread popular recognition of the opioid epidemic is relatively recent, the Mexican government has recognized the concern for more than a decade. A former Mexican ambassador to Beijing describes the issue:

> When Jorge Guajardo arrived in Beijing as Mexican ambassador in 2007, he came with a directive about what was his country's most urgent issue with the Chinese government. Mexico needed China to curb its manufacturing and sale of a dangerous class of chemicals—precursors to making fentanyl and other synthetic drugs—that flowed nearly unchecked into North America. . . . Drug cartels in Mexico used the China-made chemicals to fuel their growing arsenal of heroinlike synthetics sold into the United States to feed the country's hunger for opioids. For six years, his tenure as ambassador, Guajardo tried to get China's government to stop production of the chemicals powering the deadly epidemic. . . . "Every single time, the Chinese would shrug and say, 'We don't know what you're talking about'," he recalled. "They never wanted to pay attention to it."[25]

Fitting the profile of attribution evasion, the nexus between Chinese government, opioid production, and Mexican cartels provides a perfect example of actions that cross multiple domains, making attribution, let alone response, very challenging. The opioid epidemic is so severe that it has led to a decline in American life expectancy and labor participation rates, compounding adverse societal impacts.[26] Beyond these implications, something far more wicked could be in play: American opioid deaths may not simply be the unintended consequences of legitimate pharmaceutical production but part of a larger design to compromise the social fabric of the United States.

American addiction to Chinese products is not limited to opioids and their derivatives. "Made in China" is a ubiquitous label in the United States; Americans are accustomed to cheap, throwaway Chinese products, as well as high-tech products such as smartphones, televisions, and other appliances.[27] American consumption of Chinese goods has not only led to a massive trade deficit, but there is another much more concerning dependency that has been created: the U.S. military's industrial supply chain has many Chinese producers at its base.[28] As reported in *Financial Times*, "China represents a significant and growing risk to the supply of materials and technologies deemed strategic and critical to US national security."[29]

Despite the fractious U.S.-Chinese trade battles in 2019, American companies continue their addiction to the massive and growing Chinese consumer market, as illustrated by Walmart's declared intent to invest $1.2 billion in its

Chinese distribution centers.[30] The lure of Chinese market share comes with challenges and stipulations, most notably in requirements for Chinese-majority joint venture (JV) and the transfer of intellectual property (IP):

> First, the Chinese government uses foreign ownership restrictions, such as formal and informal JV requirements, and other foreign investment restrictions to require or pressure technology transfer from U.S. companies to Chinese entities. These requirements prohibit foreign investors from operating in certain industries unless they partner with a Chinese company, and in some cases, unless the Chinese partner is the controlling shareholder. Second, the Chinese government uses its administrative licensing and approvals processes to force technology transfer in exchange for the numerous administrative approvals needed to establish and operate a business in China.[31]

Here again, we witness the wisdom of Sun Tzu: "Thus, those skilled at making the enemy move do so by creating a situation to which he must conform; they entice him with something he is certain to take, and with lures of ostensible profit, they await him in strength."[32] Although Sun Tzu is considered a military philosopher, the above comment could be applied in a variety of domains—including economic. Economic warfare has many adaptations, such as coercion (as mentioned previously with Gazprom), market enticement, and the theft of intellectual property.

Concerns regarding the transfer of intellectual property are not limited to Chinese government transfer from foreign companies that want to do business in China. Eric Rosenbaum of CNBC reported, "One in five North American-based corporations on the CNBC Global CFO Council says Chinese companies have stolen their intellectual property within the last year."[33] Disturbingly, the theft of American intellectual property seems to follow a theme similar to that of China's opioid production. A Washington-based U.S. trade lawyer with 30 years of experience in the field told *Asia Times*, "We can raise tariffs, have high-level meetings, sign memoranda of eternal understanding and eternal friendship, but [China] will not change." He continued, "Their policies favoring *theft of intellectual property on an industrial scale* have contributed to the greatest wealth transfer since the Iranian-Arab creation of the OPEC cartel raised the price of energy in the West."[34]

Emergent Dynamics of Social A2/AD

It is time to seriously assess the changing character of conflict and consider the steps necessary to ensure the American and Western democratic societies succeed in this type of nonkinetic war. Interestingly, the SARS-CoV-2 (COVID-19) pandemic presents compelling lessons and opportunities to address the threats posed by social A2/AD.

Supply chain challenges were quickly evident as Americans (and presumably others) rushed to buy surgical and N95 masks. This rush to stockpile quickly expanded to toilet paper, cleaning supplies, and bread and other foodstuffs, among other things. This rush for masks (and other medical supplies) impacted the medical and first responder communities—the people who need them most. With approximately 80 percent of medical masks made in China, and the Chinese government consuming and buying all the masks made in China, the United States struggled to manufacture these masks domestically.[35] The U.S. government invoked the Defense Production Act of 1950, a Cold War-era mobilization mechanism, to increase production of existing production capacity while speeding the conversion of other domestic manufacturing facilities.[36] As Americans adapt to the COVID-19 outbreak, there is growing realization that the United States is held hostage by Chinese manufacturing. This extends beyond masks and into other life-critical items, such as pharmaceuticals and the previously mentioned concerns with the U.S. military supply chains.[37] Simply stated, China can—and is—holding lifesaving equipment back from the United States during this outbreak. China's motivation can be debated but not the actions.

COVID-19 is also proving that accurate and up-to-date information at national and global levels is vital. Certainly, the rush to hoard masks and toilet paper derived from a lack of information and understanding that fostered perceptions that led to panic buying and purchasing habits. Despite this, the most compelling information discussion is the narrative being used by China, Russia, and others that the United States is the cause of the virus: "In the case of China, Russia and several other countries, however, misinformation is deliberately being spread by state media to deflect criticisms of their government actions, or lack thereof, and to push the blame onto someone else."[38] Of additional note is the suppression of information, especially concerning China's published time line of the virus outbreak.[39] Chinese foreign ministry official Zhao Lijian took to twitter saying, "CDC was caught on the spot. When did patient zero begin in US? How many people are infected? What are the names of the hospitals? It might be US army who brought the epidemic to Wuhan. Be transparent! Make public your data! US owe us an explanation!"[40] This information battle has included Chinese protests about references to the virus as the Wuhan Virus, with declarations of racism, not just from Chinese officials, but from American outlets as well.[41] The information campaign took on a different dynamic in Italy, where China allocated modest amounts of medical supplies and staff to assist in Italy's COVID-19 response. As Alessandra Bocchi of the *Wall Street Journal* points out,

> these acts are not as altruistic as they might appear. The major-

> ity of ventilators shipping to Italy are from the Chinese company Mindray, which sells its products at a lower price than its global competitors. China has a surplus of medical equipment now that the outbreak appears to have reached its peak there. Demand is rising elsewhere as the virus spreads, so Chinese companies are ramping up production to gain global market share.[42]

When taken together, the socioeconomic and information dynamics created by COVID-19 look like a Chinese social A2/AD strategy in a box. The true opportunity for the United States and our allies is the unmasking of China's nonmilitary levers of power. From supply chain prowess (and corresponding dependency of the United States and others) to its information strategy, the world has seen that China will act rapaciously in its attempt to control both materials and information, using them as weapons to gain power, influence, and market share. The COVID-19 outbreak has—unintentionally—given the world a view of how China might use various mechanisms to coerce others for their advantage—or worse.

Counterstrokes

Besides the COVID-19 example, some recognition of the threat by social A2/AD-like concerns have been made in recent years. Many cyberattacks have been attributed to Russia and China (among others); Russian election tampering is recognized, attributed, and countermeasures have been taken; Chinese unfair business practices and intellectual property theft is common discussion in national security and corporate circles and is a core element of ongoing U.S.-China trade discussions; and the Committee on Foreign Investment in the United States has dramatically increased its China-related agenda items and has been reinforced by the Foreign Investment Risk Review Modernization Act of 2018.

Although significant, these steps need to be expanded in scope and depth, with specific attention paid to nefarious actions designed to compromise the U.S. and Western domestic environments. Recognition that Chinese and Russian information and economic entities are fundamentally agents of their respective governments is paramount. Gazprom, ZTE, and Huawei (among scores of others) meet allegations of government control with a well-rehearsed chorus of denials arguing that they are not agents of the state.[43] Despite these protests, there is little question that—even if not the current "arrangement"—Putin and Xi Jinping have the ability and will to weaponize Russian and Chinese information and economic outputs to support national agendas.[44] On the heels of recognizing the threat presented by social A2/AD, there must be a comprehensive, competitive strategy designed to defend against and counter malicious incursions. This approach is characterized by Thomas Mahnken through five features:

> First, it presupposes a concrete, sophisticated opponent. . . . Second, the competitive strategies approach assumes interaction between competitors. . . . Third, the competitive strategies approach acknowledges that the choices competitors have open to them are constrained. . . . Fourth, the competitive strategies approach acknowledges that interaction may play out over the course of years or decades. . . . Finally, the competitive strategies approach assumes sufficient understanding of the competitor to be able to formulate and implement a long-term competitive strategy, a task that requires not only an understanding of what a competitor is doing, but also why he or she is doing it. Effective competitive strategies are predicated on an understanding of a competitor's decision-making process and doctrine.[45]

The prescription that Mahnken details requires a level of study, detail, coordination, resource allocation, and commitment that describe a great challenge for the United States and our allies. As one witnesses the dysfunction of political discourse throughout the Western world, it is difficult to envision a strategy of substance being developed, let alone one that is properly resourced and effectively executed across decades. This challenge comes at a time where continuing resolutions are more frequent than actual budgets, just as debt, deficit, and nondiscretionary spending continue to grow, leaving an ever-shrinking portion of federal outlays to manage the business of government operation and national security.

Social A2/AD attacks are a national security concern. Unlike past threats to national security, the response to social A2/AD incursions is generally not a military one. As it is fundamentally an attack on society, the response must start as a social one. First and foremost, U.S. leadership (from a national level down to to municipal and community levels) needs to realize that they are often the unwitting pawns by furthering divisive rhetoric, functionally serving as this century's "useful idiots." Indeed, none other than former sectary of defense and U.S. Marine Corps general James N. Mattis considers American tribalism as the chief threat to the nation.[46] Economic entities must also recognize that the search for profit can lead to negative implications, as has been illustrated repeatedly. There must be fundamental recognition that a strong *Western* free market economy is to their benefit; short-term thinking for immediate return from growing Chinese markets only digs a deeper hole.[47] These are uncomfortable discussions to have with domestic and allied corporations, publics, and present immediate costs. There is risk but risk that is visible. The longer that the "invisible" risk engendered by social A2/AD is denied, the harder it will be to recover—the so-called slow boil of the frog. There are, however, opportunities. Why not combat Huawei's 5G development in Europe through a multinational corporate effort bringing Ericsson, Nokia, and Cisco together to form a high-quality, cost-effective counter to Huawei's advances? Further, as some have suggested that 5G is a national security issue, there should be a discussion of a public-private partnership that removes *some* of the cost and risk from private companies.[48] It is recognized that there are many legal challenges (domestic and international) with such proposals, but creative solutions are necessary as we lurch forward into the twenty-first century's unknowns. A safe information domain is critical to national and individual security and liberty. Considering existing information domain risks, it is easy to envision a much higher cost if authoritarian-directed corporations dominate the international 5G network.

Conclusion

Social A2/AD presents a critical threat to the United States. It is often said that the only way to beat America is from within. The threat presented through the sociopolitcal and socioeconomic means, described as social A2/AD, illustrates the concern. Inherently opaque, social A2/AD is easy to dismiss and difficult to ascribe to any particular source. It must be viewed through a comprehensive lens, not as discrete actions. Social A2/AD recognizes nonmilitary activities designed to deny an adversary the ability or will to act or respond. Social A2/AD creates and exploits social fissures to the point where the target society is so fractured that response is prevented due to internal dynamics that impede, distract, or preoccupy the instruments of governance. The building of these social fissures is multifaceted (economic, informational, illicit) and dynamic, in many ways facilitated by social media, which is an ideal medium for propaganda and disinformation with masses of willing, ignorant, and unwitting propagators. All these pathways are designed to exploit societal vulnerabilities just as they are concealed by counter narratives and legal obfuscation, exploiting and challenging the high standard of legal clarity that is necessary for decisive response. Indeed, ever-threatened Taiwan recognizes the threat presented by social A2/AD: "The main worry of military planners here isn't so much a full-scale amphibious invasion. Rather, they fear the mainland sowing chaos and disrupting the economy as a way of trying to bring Taiwan to heel."[49]

The aggregate effect of the multitude of social A2/AD attacks could be disastrous for the United States and our allies. The combined effect, over time, of unattributed or unrecognized actions—some with the perception of benefit—is irresistible. It is critical that the United States, along with our allies and partners, realize that China and Russia already act as though they are in great power *conflict* with the United States, using nonmilitary means as their weapons. Many may not wish to believe this the case, but the comprehensive view of Russian and Chinese activities illustrates strong adversarial strategies against the United States. To misappropriate Joseph Heller from *Catch-22*, "Just because [you are not] paranoid doesn't mean they aren't after you."[50]

Endnotes

1. For discussion of Chinese A2/AD, please see Matthew Jamison, "Countering China's Counter-Intervention Strategy," Strategy Bridge, 11 August 2020; and Ngo Minh Tri, "China's A2/AD Challenge in the South China Sea: Securing the Air From the Ground," *Diplomat*, 19 May 2017.
2. Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Knopf, 2007), 269–307.
3. Pease see *Insurgencies and Countering Insurgencies*, Field Manual 3-24 (Washington, DC: Department of the Army, 2014).
4. *National Security Strategy of the United States of America* (Washington, DC: White House, 2017).
5. "The Fulda Gap represented the shortest route (through the cities of either Fulda or Giessen) from the border between East Germany and West Germany to the Rhine River. Throughout the Cold War, North Atlantic Treaty Organization (NATO) and Warsaw Pact military forces remained heavily concentrated in the area. Constant patrols, surveillance, and alerts were carried out along the border, where opposing observation points stood less than 100 yards apart, until the reunification of Germany in 1990." For an explanation of the Fulda Gap during the Cold War, please see "Fulda Gap," Britannica, 19 December 2018.
6. The term *social A2/AD*, although not a one-for-one analog to antiaccess/area-denial, was selected due to its functional utility in inhibiting, or preventing altogether, a nation's ability to respond to an adversarial act. If a country is unable or unwilling to respond, A2/AD has been achieved.
7. Doug Livermore, "China's 'Three Warfares' in Theory and Practice in the South China Sea," *Georgetown Security Studies Review*, 25 March 2018; Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, 30 January 2018; and "US Needs China More Than China Needs the US," IndustryWeek, 6 April 2018.
8. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford, UK: Oxford University Press, 1963), 77.
9. Sun Tzu, *The Art of War*, 84.
10. William M. Mott IV and Jae Chang Kim, *The Philosophy of Chinese Military Culture: Shih vs. Li* (New York: Palgrave MacMillan, 2006), 11.
11. Michael Howard and Peter Paret, eds. and trans., *Carl Von Clausewitz: On War* (Princeton, NJ: Princeton University Press,1984), 485–86, 495–96.
12. Howard and Paret, *Carl Von Clausewitz*, 595–96.
13. Jessica Brandt and Torrey Taussig, "The Kremlin's Disinformation Playbook Goes to Beijing," Brookings, 19 May 2020.
14. Katie Simmons, Bruce Stokes, and Jacob Poushter, "NATO Publics Blame Russia for Ukrainian Crisis, but Reluctant to Provide Military Aid," Pew Research Center, 10 June 2015.
15. Gabriel Collins, *Russia's Use of the "Energy Weapon" in Europe*, Baker Institute for Public Policy Issue Brief (Houston, TX: Rice University, 2017).
16. Kristin Huang, "Why China Buying Up Ports Is Worrying Europe," *South China Morning Post*, 23 September 2018; Eric Reguly, "China's Piraeus Power Play: In Greece, a Port Project Offers Beijing Leverage over Europe," *Globe and Mail*, 7 July

2019; and Joanna Kakissis, "Chinese Firms Now Hold Stakes in Over a Dozen European Ports," NPR, 9 October 2018.

17. Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," *New York Times*, 25 June 2018.

18. See Owen Churchill, "China Hasn't Changed Belt and Road's 'Predatory Overseas Investment Model', US Official Says," *South China Morning Post*, 13 September 2018; Cheang Ming, "China's Mammoth Belt and Road Initiative Could Increase Debt Risk for 8 Countries," CNBC, 5 March 2018; and Jeff Smith,*China's Belt and Road Initiative: Strategic Implications and International Opposition* (Washington, DC: Heritage Foundation, 2018).

19. "Assessing China's Digital Silk Road Initiative," Council on Foreign Relations, accessed 30 March 21; and Nyshka Chandran, "Surveillance Fears Cloud China's 'Digital Silk Road'," CNBC, 12 July 2018.

20. Josephine Ma, "US and China Escalate Huawei Feud in Europe with Warnings to Germany and Poland," *South China Morning Post*, 12 March 2019; and Steve McCaskill, "UK May Reconsider Huawei Ban," TechRadar, 13 August 2019.

21. Special Counsel Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, 2 vols. (Washington, DC: Department of Justice, 2019).

22. Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money* (New York: Institute of Modern Russian, 2014), 6.

23. Douglas Rushkoff, "How We All Became Russia's 'Useful Idiots'," Medium.com, 5 December 2018.

24. Greg R. Lawson, "The Fentanyl Crisis Is a Reverse Opium War," *National Interest*, 26 December 2017; and Vicky Yates Brown Glisson, "America Is in an Opium War for the 21st Century," Real Clear Policy, 22 March 2019.

25. Kathleen E. McLaughlin, "China Killed Prince: Fentanyl Is the PRC's Deadliest Export—and New Promises Probably Won't Stop It," *Foreign Policy*, 7 December 2018.

26. Rob Stein, "Life Expectancy Drops Again as Opioid Deaths Surge in U.S.," NPR, 21 December 2017; and Brennan Hoban, "The Far-Reaching Effects of the US Opioid Crisis," Brookings, 25 October 2017.

27. See also Heather Somerville, "China's Penetration of Silicon Valley Creates Risks for Startups," Reuters, 28 June 2018.

28. Gina Heeb, "Trump's Favorite Scorecard for the US-China Trade War Took a Hit in July," Business Insider, 4 September 2019.

29. Katrina Manson, "Trump Attacks Chinese Control of Military Supply Chains," *Financial Times*, 5 October 2018. Note: comment from *Executive Order 13806, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (September 2018) as quoted by Manson.

30. Laura He, "Walmart Is Investing $1.2 Billion in China," CNN, 4 July 2019.

31. *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* (Washington, DC: Office of the United States Trade Representative, 2018).

32. Sun Tzu, *The Art of War*, 93.

33. Eric Rosenbaum, "1 in 5 Companies Say China Stole Their IP Within the Last Year: CNBC CFO Survey," CNBC, 1 March 2019.

34. Grant Newsham, "U.S. Helpless against China's IP Theft," *Asia Times*, 2 April 2019. Emphasis added by author.

35. Pamela Boykoff and Clare Sebastian, "With No Shipments from China, Medical Mask Suppliers Have to Choose Whom to Supply," CNN, updated 6 March 2020.

36. "DOD Announces $74.9 Million in Defense Production Act Title III COVID-19 Actions," Department of Defense, 4 December 2020.

37. Yanzhong Huang, "U.S. Dependence on Pharmaceutical Products from China," Council on Foreign Relations, 14 August 2019.

38. Joseph Micallef, "Blaming America: China Weaponizes Misinformation About COVID-19," Military.com, 23 March 2020.
39. Please note that while the Axios.com time line begins in December, Chinese accusations point at U.S. soldiers introducing the virus to China in October 2019, indicating awareness well before December. Bethany Allen-Ebrahimian, "Timeline: The Early Days of China's Coronavirus Outbreak and Cover-up," Axios, 18 March 2020.
40. Zhao Lijian, as quoted in Ben Westcott and Steven Jiang, "Chinese Diplomat Promotes Conspiracy Theory that US Military Brought Coronavirus to Wuhan," CNN, updated 13 March 2020.
41. See Joseph Wulfsohn, "CNN Blasted for Now Declaring 'Wuhan Virus' as 'Racist' After Weeks of Network's 'China's Coronavirus' Coverage," Fox News, 12 March 2020; and Marie Myung-Ok Lee, " 'Wuhan Coronavirus' and the Racist Art of Naming a Virus," Salon, 7 February 2020.
42. Alessandra Bocchi, "China's Coronavirus Diplomacy," *Wall Street Journal*, 20 March 2020; and Theresa Fallon, "China, Italy, and Coronavirus: Geopolitics and Propaganda," *Diplomat*, 20 March 2020.
43. Lindsay Maizland and Andrew Chatsky, "Huawei: China's Controversial Tech Giant," Council on Foreign Relations, updated 6 August 2020; Lingling Wei, "China's Xi Ramps Up Control of Private Sector. 'We Have No Choice but to Follow the Party'," *Wall Street Journal*, 10 December 2020; and Macey A. Bos, "Gazprom: Russia's Nationalized Political Weapon and the Implications for the European Union" (master's thesis, Georgetown University, 2012).
44. Tom Mitchell and Xinning Liu, "Chinese Communist Party Asserts Greater Control over Private Enterprise," *Financial Times*, 28 September 2020; Wei, "China's Xi Ramps Up Control of Private Sector"; and Bos, "Gazprom."
45. Thomas G. Mahnken, ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice* (Stanford, CA: Stanford University Press, 2012), 7–8.
46. Jim Mattis, "Jim Mattis: Duty, Democracy, and the Threat of Tribalism," *Wall Street Journal*, updated 28 August 2019.
47. "US Needs China More Than China Needs the US"; and "China and the NBA Are Coming to Blows over a Pro-Hong Kong Tweet. Here's Why," Business Insider, 22 October 2019.
48. Please see *The National Security Challenges of Fifth Generation (5G) Wireless Communication: Winning the Race to 5G, Securely* (Arlington, VA: Intelligence and National Security Alliance Cyber Counsel, 2019).
49. Nicholas Kristof, "This Is How War with China Could Begin," *New York Times*, 4 September 2019.
50. Joseph Heller, *Catch-22* (New York: Samuel French, 1971). The original quote was "Just because you're paranoid doesn't mean they aren't after you."

Representation of Armed Forces through Cinematic and Animated Pieces
Case Studies

Michael Cserkits, PhD

Abstract: In this article, the author will examine the representation of armed forces in cinematic productions and anime, with case studies of the United States and Japan. The sample will consist of a movie that has a clear involvement of the United States armed forces and of an anime series that was cofinanced by the Japanese Self-Defense Forces. The analytical method used will be textual analysis, in combination with videography, a method that supports interaction analysis of moving images. In comparing those two different approaches of the armed forces of Japan and the U.S. military, the author hopes to shed light on not simply the representation of the groups but also desired self-identification of the respective armed forces.

Keywords: propaganda, cinema, videography, Japan, U.S. military

Introduction

The scope of this article is to present selected case examples of representations of different armed forces. The examples differ not only from their modus operandi—as on the U.S.-North American side the material analyzed will be a mainstream cinematic movie (*Transformers 4: Age of Extinction*), and on the Japanese side an animated series (*Gate: Thus the JSDF Fought There!*)—but also on the historical background of these two opposite cases. The reason for choosing such different examples lies in the same logic that

Maj Michael Cserkits, PhD, serves in the Austrian Armed Forces and is an independent postdoctoral researcher. He graduated from the Austrian Military Academy, holds an MA in sociology, an MA in social and cultural anthropology, and a PhD in African studies. He is currently working in the research fields of military sociology/anthropology and security issues relating to the Sahel zone.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201008

they use, as this article will illustrate during the analysis. The United States, as one of the victors of World War II and as a still uncontested military power in the globalized world, has developed an impressive industrial-cinematic complex with a startling—and sometimes even tense—history of cooperation, which will be shortly explained in the subsequent section. This complex will be compared with Japan, which can be seen as its counterpart when it comes to military history. After being on the losing side of World War II, Japan has developed its own unique way of distributing and presenting the Japanese Self-Defense Forces (JSDF) in a civilian context, with the use of anime movies and series.

Both sides, as this article argues, have different ways in presenting their armed forces to a civilian audience. But even though there are so many differences in culture, language, and presentation style, they are both trying to reach the same goal: gain popular domestic support and backup for their soldiers, regardless of their tasks or missions.

The Japanese Side

On the Japanese side, Christopher Hughes argues that the JSDF have become more popular and fashionable through their "manga-ization," especially in recruitment materials.[1] The JSDF have also managed to mediate security threads for Japan through a narrative in special anime, such as Kantai Korekushon (Japanese: 艦隊これくしょん; English: Kantai Collection) with a focus on the maritime dimension of the JSDF, which aired in 2015.[2] Takayoshi Yamamura has traced the cooperation between the JSDF and anime producers back to the 1980s, beginning with a call for more realism in anime, but "it was not until the year 2000 that JSDF began publicly collaborating with the production of anime, and JSDF began actively collaborating with televised anime from around 2003 to 2004."[3] After several attempts and series, which all created only a low level of feedback, the series *Gāruzuando Pantsā* (Japanese: ガールズ & パンツァー; English: Girls and Panzer) was the first hit that brought a shift in the image of the JSDF in 2012 to a more popular and sophisticated image, immediately followed by *Gate: Jieitai Kano Chi nite, Kaku Tatakaeri* (Japanese: ゲート自衛隊彼の地にて、斯く戦え; English: Gate: Thus the Japanese Self-Defense Force Fought There!) in 2015 and *Haisukūru Furīto* (Japanese: ハイスクール・フリート; English: High School Fleet) in 2016, the latter providing immense public relations support for the Japanese Maritime Self-Defense Forces (JMSDF).[4] Even if the highly sexualized representation of younger girls in such productions has been subject to academic critique, the current literature shows no traceable negative consequences for the JSDF as whole.[5]

> At most, the aim seems to be to gain topicality and to enhance the popularity of JSDF. In other words, the campaigns act as

> nothing more than another avenue for publicity in order to get the attention of younger generations and instill in them a sense of familiarity towards JSDF.[6]

This approach by Japan is a clever use of smart power (an attempt that combines soft and hard power in an innovative way), where Japan ranks eighth in the world and the United States fifth, a term first introduced by Hillary R. Clinton in 2009 during her nomination hearing to be secretary of state.[7] As Yee-Kuang Heng has noted, smart power is seen in Japan not only as a tool for the state, used in an integrated or comprehensive approach led by the national grand strategy, but rather a tool that is used by the JSDF, contributing to promoting a helpful and friendly image around the world.[8] As missions abroad are not the primary tasks for the JSDF (contrary to the distinct expeditionary character of the U.S. forces), those smart power strategies are not as well documented as the domestic communication regimes that are dominating contemporary Japan. Following the study of Sabine Frühstück, where she stated that the Japanese Ministry of Defense had first "symbolically 'disarmed' the Self-Defense Forces; normalized and domesticated the military to look like other (formerly) state-run service organizations such as the railways and postal systems" back in the 1970s, the current shift to a remilitarization of the Japanese Self-Defense Forces has clear strategic impacts due to the position of Japan, bordering a revitalized Russia in the north and a rising China in the west, not to mention a still unpredictable North Korea in its immediate neighborhood.[9] Although a distinct militarization and rework of war memories has not fully encompassed the whole of society, JSDF has "benefitted from the utilization of popular culture, which enhances intimacy towards JSDF, particularly among young people."[10] This intimacy nurtures nationalism, as it reshapes images and symbols from their original historical context and replace it in a more suitable discursive way.[11] This practice is known as *invented tradition*, a term introduced by the historians Eric Hobsbawn and Terence Ranger:

> "Invented tradition" is taken to mean a set of practices, normally governed by overtly or tacitly accepted rules and of a ritual or symbolic nature, which seek to inculcate certain values and norms of behavior by repetition, which automatically implies continuity with the past. In fact, where possible, they normally attempt to establish continuity with a suitable historic past.[12]

By creating a connection between certain aspects of the historic past and explicitly concealing other aspects of this epoch, continuity is produced to be used or even abused.

As previously mentioned, the examined anime series will be *Gate: Jieitai Kano Chi nite, Kaku Tatakaeri* as it clearly depicts the above-mentioned trends as well as several attempts to reshape the Japanese past when talking about its armed forces. Its unique selling point, which makes it so interesting, is that it solely deals with the JSDF, its tactics, techniques, and procedures as well as a scripted picture of everyday life as a soldier. Contrary to *High School Fleet*, *Arpeggio of Blue Steel*, *Kantai Collection*, or others, the main character of the series is not a young girl or a group of young girls, but a fully grown officer in his mid-30s in the JSDF with a credible background story and social life as well. Notably, Paul Martin has also analyzed the same anime, but with a clear focus on the connection between the series and Japan's rising nationalism.[13]

The United States' Side

The intense bond between the military and the U.S. industrial complex was first built during World War I, when private firms were contracted to design the first aircraft.[14] Although the aspect of the closer cooperation between the cinematic complex and the Department of Defense (DOD) is a topic worth exploring, there already exists a vast literature about this theme, and it would be beyond the scope of this article. After the end of World War II, concerns about Communist filmmakers in Hollywood led to a quarrel between those two components, which lasted until the first high-budget production was released with support from the Pentagon with *Top Gun* in 1986.[15] Since then, there has been a shift in the military-cinematic-industrial complex. Additionally, the target audience changed during the last 60 years, from a diversified mission in the beginning, such as military documentaries for educating specific audiences or movies produced in foreign-occupied territories to promote American values and ideas, to a straightforward target audience committed to the use of military means as legitimate and necessary, strengthening the reputation of the armed forces and helping to recruit new soldiers.[16] With the blockbuster *Transformers* in 2007, the cooperation between DOD, Hollywood, and the merchandising industry reached a new level.

For critical literature regarding the *Transformers* movie, several authors had already stated their concern that since the first cooperation in 2007 between the Pentagon and the movie industry in Hollywood, an effective but dubious collaboration emerged: "The synergies of the Paramount-Pentagon partnership were simple but powerful—free high-tech stage props in exchange for a two-hour recruitment advertisement for the military."[17] This partnership proved useful, as *Transformers* was just one of a series of civil-military movie cooperations that would occupy the big screens of cinemas all over the world, starting with *Iron Man* to *GI Joe* and several others. This symbiotic relationship would not stop at the screen but rather reach much deeper into society, as William Hamilton has pointed out clearly: "Today's troops effectively received basic training as children."[18] Apart from making young teenagers familiar with the military and its capability, since the deepening of the cooperation between Hollywood and the Pentagon, controversial political messages are no longer welcome and might even be cut out of the script.[19]

But does this political agenda apply to the whole *Transformers* series? Tanner Mirrlees had analyzed the first two movies, *Transformers* and *Transformers: Revenge of the Fallen*, where she comes to the conclusion that the main profiteer of these two action movies was the DOD, as installations (e.g., Air Force bases) worked as shooting scenes and backgrounds, and almost all modest-to-middling characters (e.g., tourists, soldiers, or guards) were played by real soldiers or ex-military personnel.[20] However, not only did the DOD gain positive feedback out of the cooperation, it could also present its newest technological advances, declare the ongoing wars as Joint operations (as the Navy and Air Force support the troops on the ground in exotic places), and further boost recruitment activity. As for *Transformers: Age of Extinction*, it was the first movie where the Chinese Movie Channel had invested lots of effort (and money) in it to secure its success on mainland China, despite heavy critique from the United States due to the growing Chinese influence in the plot and some semipolitical messages, which presented the Chinese officials as brave and benevolent.[21]

Another aspect of the movie in the recent literature are the characters, Autobots and Decepticons, themselves. Harlon D. Wilson assumes that the robotic violence in the movie is a vehicle for sexuality, where "transformers collectively function as a channel for technomasculine desire and American sociocultural production."[22]

Methodology

The methodological approach will be presented via an audiovisual research agenda. As Hubert Knoblauch et al. point out, "video has become a medium that pervades our everyday life."[23] On the one hand, the way of producing the situational arrangements *that the producer wants us to see* has a huge impact on the message that is transported via synchronic elements of vision and sound. On the other hand, editing is also a very important method for further analysis. Knoblauch et al. call this "recipient design."[24] Therefore, this article considers that it is analyzing edited cinematic products and will first classify them as highly selected and as very reactive, as it is unlikely that situations in the films happened exactly in the presented time frame.

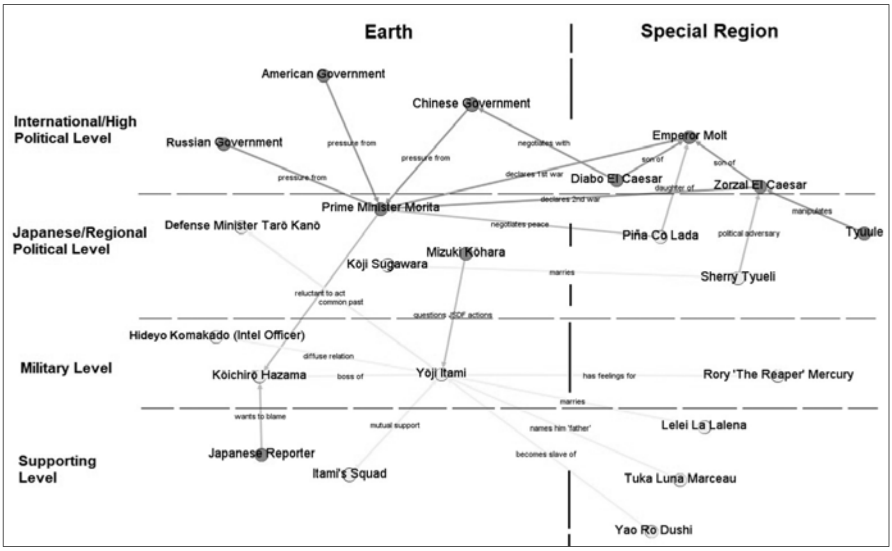
To handle these fundamental elements, which are embedded in the nature of video, Knoblauch and Bernt Schnettler invented a method for video analysis, which they call *videography*.[25] Videography consists of three main elements, though for this analysis only the first two steps are relevant: first, a descriptive approach that considers all visible elements seen in the video as well as the modes of production, at least those that can be reconstructed. This comes closest to the mode of a close reading or textual analysis when compared to written material. In this first step, a detailed transcription of the respective scene is produced, giving special emphasis on cut scenes, background music, and the arrangement of the actors. Second, the focus of the analysis switches to the "interaction taking place in a certain social situation."[26] The content may be fictional, but to be understood by the audience, the editors and producers have to rely on replicable social interactions that are nonfictional, with the possibility of creating new belief systems or myths. As the figure and uniform of a soldier may vary in degrees between Japanese and American points of view, both audiences have certain expectations about their behavior, their role in society, and the purpose of serving their country. In varying these expectations to different degrees, the producer can build a role model from scratch and highlight socially expected or anticipated behavior, while neglecting other (but nevertheless given) parts. The comparison with a ray of light may be useful to describe this method: As light consists of different colors, the animation or cinematic context works as a prism, filtering special colors out while reinforcing others. Features (sound, picture, speech) of videos, movies, and anime appear simultaneously, so a descriptive approach is necessary to gather as much information as possible to create a dense description of what is seen by the viewer. As for the constraints of this approach, the analyzed source is already edited, shaped, and formed, and is respectively fictional, especially for the animated part of the material. Videography is therefore applicable, as although the protagonists are not real, their messages are, and they are embodied in the editing process, which will be traced and examined.

Analysis of *Gate*

As for a short synopsis of *Gate*, the main plot deals with a mystical portal (the Gate), which opens in the middle of Tokyo. Soon after this interdimensional tunnel had opened, a mystical and medieval equipped army attacks Japan, but it is shortly defeated when the JSDF launched its counterattack. After establishing a forward operational base, which will later be a city called Alnus Hill, the Japanese government named the fairy world the "Special Region." The series revolves around the main character, Yōji Itami, a first lieutenant who will lead a reconnaissance team to the Special Region.

Regardless of the plot or even the fictional character of the series, figure 1 already shows the main narrative that is deeply rooted within the show. As shown, most adversaries or evil characters are located above the military level. In this case, the only political players that remain trustworthy during the show

Figure 1. Relationships in *Gate*, illustrated with Network-Analysis (light gray=partner; dark gray=adversary)



Source: Courtesy of author, adapted by MCUP.

are the minister of defense and the special representative of Japan located in the Special Region, a young diplomat named Kōji Sugawara, who puts his life in danger when giving political asylum to one of Zorza El Caesar's (son of the emperor and later the emperor) political adversaries. There are no malcontents in the supporting or civilian level and all their intentions are clearly outspoken with no hidden agenda, making them the perfect population for civil-military cooperation (CIMIC), quickly repairing all of the damage that has been done during the first counterattack of the JSDF.[27] For example, after Itami and his squad are trapped in a city near Alnus Hill, which is under siege of local bandits, they order an air strike. However, to prevent casualties, the JSDF just send a Bell AH-1 Cobra attack helicopter, which wipes out the enemy. After arriving over the sky of the besieged city, the following dialogue occurs:

> (12:47) Hamilton Uno Ror: "It's a monster." ["Ride of the Valkyrie" music starts]
>
> Piña Co Lada: "A flying horse of steel? How can this even exist? No soldier or army can match such a level of force! How it can eradicate everything. No pride, no glory, nothing left in its wake." [Helicopter begins to shoot down people]
>
> Lelei La Lelena: "The battle is over."

> Tuka Luna Marceau: "It got every last one of them?"
> Piña Co Lada: "Does the goddess really think this low of us? Are we really so small? So insignificant?"
> JSDF-soldier 1 (ropes down from another helicopter): "Go, go, go. Clear the staging area for the [prisoners of war] POW. And another one for the survivors."
> JSDF-soldier 2: "Hey, Serge. I found one."
> JSDF-soldier 3: "Colonel. Yoga here. No more enemies on sight. Looks like we got a clean sweep. I'm out."
> Colonel: "All right."
> Itami: "Looks like we're done."
> Citizen: "Thank you, we are all safe thanks to you. The men in green." ["Ride of the Valkyrie" song slowly ends] "But I must ask, who are you, where are you from?"
> JSDF-soldier 3: "We are from Japan." [Catches breath and waits a second] "The Self-Defense Force." (13:56)[28]

Several elements are cleverly intertwined within this scene that deals with the concepts of help and strength. First, the propagandistic element, which is double-sided. One effect is presented toward the audience, in reference to the "Ride of the Valkyries" scene from the 1979 film *Apocalypse Now*. The second one is a cinematic element within the series, as the overwhelming combination of a helicopter attacking with famous background music (at least for people who have already engaged in movies dealing with the military) would clearly demoralize the enemy; at least, that is the scripted intent the author presumes is the effect of this scene. Given the similarity of the pictures between the helicopter formation flying to end the siege and the original composition of helicopters in *Apocalypse Now*, a reframing took place that positively underscores the power of Army aviation instead of branding it as platform of war crimes (e.g., Francis Ford Coppola's movie). Beside the propaganda element, the national pride can be traced, as it is indirectly expressed from outsiders (Princess Co Lada and her assistance), who ambivalently watch the scene with a mixture of pure angst and despair, as they now realize that they have chosen to fight such a capable adversary. Immediately after this scene, Co Lada tries to negotiate peace and convinces her father to stop the bloodshed. The third element is the CIMIC component to show the audience that the second the fighting ends, measures are taken to support the civilian population as well as the wounded enemies, just like the internationally recognized Hague Conference on Private International Law would demand. Fourth, the self-perception of the JSDF is presented through the last dialogue between a citizen and the JSDF soldier, who are referred to as "men in green." With no hesitation, even after a fight and surrounded by dead and wounded people, the soldier just states who they are, with a strong impression and stable voice.

There is no literature that describes how a modern, high-technology army would behave if they met a medieval opponent, with no offensive capabilities, vast lands, and possible resources and raw materials that are unexplored and unknown to their inhabitants. But history has shown that when two unevenly military powers collide, the stronger had no hesitation in taking advantage, no matter if it was during the scramble for Africa or the Second World War. In picturing a possible alternative, the series and its coproducer, the JSDF, wanted to give the audience an impression that the National Armed Forces are distinctively not an expeditionary or even colonial force (even if this creates a little friction, as Alnus Hill is per se a military base within extraterritorial borders). This nonexpansionistic touch can be seen as a direct approach to rewrite the very aggressive approach of Japan before and during the Second World War, suggesting that this would never happen again.

Contrary to the civilian and supporting level, the JSDF stationed in the Special Region has to frequently deal with political influence, both from the real world and the Special Region. Not only does the (reluctantly portrayed) Japanese prime minister have problems with the (belligerent) American, Russian, and Chinese presidents, these international counterparts also interfere in domestic affairs. In a trial to refurbish the first gate incident, several members of the Special Region are visiting Japan, but American, Russian, and Chinese Special Operation Forces (SOF) tried to kidnap some members of the delegation to further subdue the already-weak prime minister. Even after these SOF were all killed by Rory Mercury (a fierce 961-year-old demigoddess and apostle of Emroy, the God of Darkness, Death, War and Violence), the Japanese domestic politicians did not sympathize with the efforts of the JSDF, as the following dynamic dialogue, where Rory Mercury shall give testimony to the defeat of a Fire Dragon, who killed civilians, will show:

> (11:25) Mizuko Kōhara [interrupting Tuka Luna, raises tone of voice]: "According to the report, when the dragon attacked, it killed one hundred and fifty people fleeing the village. But not a single soldier was killed or injured during that engagement." [camera starts spinning around her]. "The Self-Defense Force is supposed to risk their lives and fight for those in danger. But here, they chose to run from that fight and it costs people their lives!" [Camera switches back to Rory, who frowns, then immediately switches back to Mizuko, she screams] "SO YOU NEED TO TELL US EVERYTHING. Tell us what you saw, tell us what they did! Tell us the truth!"

Rory Mercury [camera switching back to Rory, she takes a big breath and screams]: "ARE YOU A GOD DAMN IDIOT?" [People holding their ears]

Mizuko Kōhara: "Huh? Excuse me?"

Rory Mercury: "I believe you heard my question. You are probably asked that a lot. Little Miss Thing." [smiles]

Mizuko Kōhara: "You speak Japanese?"

Rory Mercury: "Well, look who just caught up. I assume what you really want to know is how Itami and his people fought against the dragon, am I right?" [Cutback of the events] "They did everything they could, and then, so, they did not hide in their carriages nor behind any civilian. I tell you they did nothing of this sort." [Mizuko gasps] "Let's get to the point, shall we? There are times when a soldier must protect their own life, but you sit here safe and comfortable, and accuse others of being cowards." [Camera switches toward other Parliament members who are sweating] "If you ask me, you are the coward, Little Miss Thing."

Mizuko Kōhara: "What did you call me?"

Rory Mercury: "They faced a Flame Dragon and lived to tell the tales. So, you should offer them praise for pulling off such a feat, you demonstrate a rather creative way of manipulating numbers to look a certain way, don't you? Your Self-Defense Force saved four hundred and fifty people." [Camera switching out toward livestream on Tokyo main place; cutback of the events] "I can only imagine the problems that the soldiers in this country face if THIS is how they are treated." [switchback to Rory] "Itami and his team accomplished something no one has ever done. And that is my answer to that stupid question of yours. Is that true enough for you, Little Miss Thing?" [Scene is cut by the visions of the American, Russian, and Chinese presidents who follow the trial via livestream] (23:42)[29]

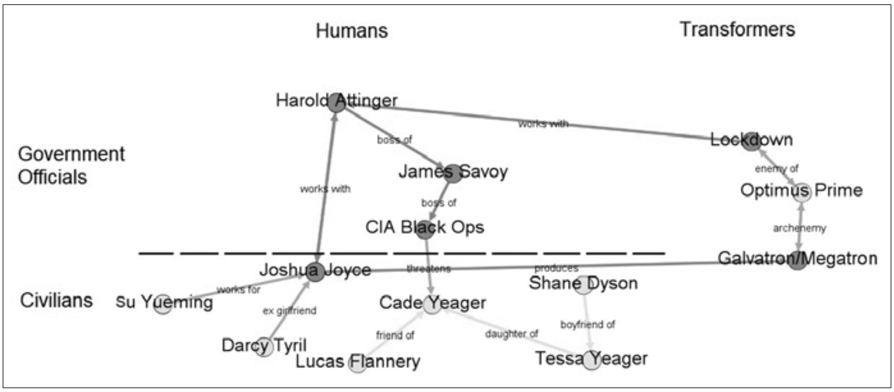
Mizuko, a member of the Japanese Parliament, is the archetype of politician in *Gate*. Even if she has never been to the Special Region, she holds a deep grudge against the military and is willing to blame them every chance she gets. She embodies a pacifist who is so eroded by hate against the military that she can no longer act with patience and is instead accusing the JSDF of acting cowardly. The element that is implemented in this scene is the paradoxical situation that Rory Mercury, a member of the Special Region with absolutely no affiliation to the JSDF, has to defend their actions and put them into the true light. Due to the series, she is portrayed as an angel of death, a servant to the Death God, so she has strong attachments and emotions regarding the fate of soldiers, which underlines an external flattery for the JSDF. The second element is the notion of deep distrust against official numbers, as she emphasizes the fact that even if people died, others had been rescued. The third element is the global perspective, where again the belligerent opponents of Japan's government had to indirectly face the accusation of Rory, which is in a broader sense directed to all politicians who have no sense of the reality of war but are eager to let others bear the costs of it.

Altogether, *Gate* offers a great variety of scenes where those two key messages are being transmitted: first, the JSDF accomplishes tremendous achievements even in the face of the greatest danger, no matter the cost. The reason for those accomplishments is up-to-date technologies and a tight and disciplined military organization, which is oriented to defending Japan and its citizens, while having no expansionistic ambitions. Second, politicians cannot be trusted (except the minister of defense, as he is portrayed as a semisoldier), no matter if they are Japanese or foreign, as they will do anything that suits their personal interest. The contrasting juxtaposition of values (soldiers with common goals and politicians with selfish, individualistic goals) is a very concerning element in the series, as it opens a possible path to undermine a democratic core institution. It casts aspersions at politicians as a whole but presents the Army as the *last democratic resort* free from corruption, and a distorted picture of the reality is presented. Another minor issue is how the JSDF presents themselves as a cultural ambassador. In doing so, the armed forces make the people of the Special Region accustomed to Japanese values, tradition, and food, and even including local citizens in the military police—a fact that is absolutely contrary to the ongoing high racial discrimination in contemporary Japan.[30] In exaggerating specific personal values and characteristics toward the audience, this series can serve as a prime example for a one-sided perception of cultural heritage and organizational values.

Analysis of *Transformers 4: Age of Extinction*

Contrary to *Gate, Transformers: Age of Extinction* (TF4) is a movie and therefore cannot offer the introduction of that many characters, plots, ploys, and intrigues. But out of the point of view of the author, it serves as another good example in dealing with propagandistic issues. As already mentioned, TF4 is a type of rogue movie (a kind of production that is per se critical to the government but not explicitly to the military) in the *Transformers* series, as it was the first who introduced a new human main character, but it is still relying on

Figure 2. Relationships in *Transformers 4: Age of Extinction*, illustrated with Network-Analysis (light gray=supporting main character; dark gray=adversaries to main character)



Source: Courtesy of author, adapted by MCUP.

old Transformers, such as Megatron or Optimus Prime. Figure 2 briefly shows the relationships between the main actors of the movie. Initially, we can see a similar picture to the Japanese case example, as again from the civilian level no real threat (with the exemption of the corrupt designer Joshua Joyce) emerges.

The main synopsis of TF4 deals with where the plot of *Transformers 3* left off, where an alien invasion almost destroyed the United States. Since then, Transformers are no longer welcome in the United States and face a deadly hunt against them by a Central Intelligence Agency (CIA) black ops team (which is already corrupted and has hijacked parts of the military; even if they do not represent the armed forces, they use them and therefore make them visible as an uncorrupted counterexample) while also being hunted by an adversary Transformer from outer space (Lockdown). The main human protagonist, Cade Yeager, stumbles accidentally into this twisted constellation and is then labeled persona non grata and has to confront himself with an ongoing conspiracy. Confronted with the already mentioned heavy Chinese influence in the movie, TF4 presents a semiofficial CIA unit called Cemetery Winds, which is an archetype of loyal, anonymous bureaucrats, putting the mission above all moral and legal aspects:

> (37:09) James Savoy: "Mister Yeager. Excuse me." [Takes off his black sunglasses] "You just said 'him'." [Looks directly into Yeager's face] "Take him down!"
>
> Cade Yeager: "What?" [Desperate music begins to play]
>
> Tessa Yeager: "Let me go! Au!" [is being pulled off by CIA member]
>
> Cade Yeager: "They don't know about the truck. I know! Just let her go!"

> James Savoy: "What kind of man betrays his brothers in flesh and blood and favors something in metal? Get this guy out of my sight!" (37:30)[31]

Savoy, portrayed as handmaiden of a higher authority (as he receives his orders via earplug from his boss Harold Attinger, the head of the CIA black ops), is, as are his fellows, completely dressed in black, symbolizing an anonymous, semifascist force that could have emerged from George Orwell's masterpiece *1984*. His loyalty to his superior has blinded him for reason and empathy, strictly carrying out commands he will obey without a doubt:

> (1:11:19) Cade Yeager: "Look, I want a lawyer, the Justice Department, somebody I can really trust. I'm just trying to protect my family. Not from your company. From the government." [Harold Attinger enters the room]
>
> Harold Attinger: "Mister Yeager. Who do you think I work for?" [smiles] [Yeager stares at him] "You are trying to protect your family. That's admirable. I'm trying to defend the nation. From alien war. We had a taste on how it looks like and we are not going to tolerate another." [sits down in front of Yeager] (1:11:39)[32]

In portraying semiofficials like Attinger or Savoy as hypocrites (both have deals with Joyce's company to retire and gain as much money out of his products as possible), they are immediately dismantled of their superior moral arguments that they are carrying like torchlights in front of them.

Important to note is the fact that the "official" military that shows up in the movie is never acting on its own but always under the auspices of Attinger or one of his subordinates (like at 1:15:03, when Attinger declares the Autobot intrusion a "CIA-military operation"). In doing so, the audience gets the impression that an already corrupt, cancer-like subdepartment is using the loyal military assets to carry out selfish tasks and is therefore neither to blame nor can it be accused of collaboration, as it was obviously betrayed during the chain of command. Again, as a rogue movie it has several aspects that declare it from the beginning as critical toward the official government, but even in such a precarious context the military remains free of any deliberately bad intentions and serves as a positive counterexample toward a corrupt and selfish secret organization that has always been suspicious by itself. A common notion of shadiness can be found in both case examples, as both—CIA and the Intelligence Officer Hideyo Komakado—are portrayed in a distrustful and creepy way.

Conclusion: Trust Politicians Only if You Must?

But what can be learned out of those case examples? As a matter of fact, both the series and TF4 have so much additional material that could be analyzed that it would fill a whole book. In this article, the main goal was to look beyond the presented fictional character and the scenes and try to figure out the main messages and ideas that are linked to cinematic products that have been produced under the eyes of the respective national militaries. Whereas *Gate* clearly serves a propagandistic aim to further boost the popularity of the JSDF, TF4 has been located in the category of *rogue movies*, a kind of production that is critical to the government, but not explicitly to the military, as it functions as an uncorrupted pure counterexample.

Both case studies have different cultural backgrounds and even their producing countries vary vastly, with the United States as a clear winner of the Second World War and currently a global power, while Japan lost the Second World War and suffered a national trauma with two atomic bomb attacks on Hiroshima and Nagasaki. But even if their history is incredibly contrary, their avenues of approaching cinematic productions are not. Both case studies clearly have shown that the primary threat to the military is not another armed force (as the JSDF could easily wipe out the whole Special Region and the Autobots had the Decepticons still under control), but merely domestic politicians opposing the armed forces, or rogue intelligence units that manipulate democratic institutions. Whether it was a cynical member of the Japanese Parliament who wanted to blame the JSDF at all cost, or an independent CIA unit that betrays the military and deliberately harms civilians alike, the threat never came out of the population or even from peers. Both productions used the scripted reality for creating a positive picture of the soldiers, its ethos, and duty toward the country, even if some of the protagonists had the chance for malpractice (e.g., Itami when a slave girl submitted herself to him). In portraying an admirable, trustworthy but somehow still down-to-earth picture of the national soldier, both productions gain support and backup for their soldiers, regardless of their tasks or missions.

National defense departments do not engage in cinematic production and sponsor them with generous grants, knowledge, and access to military installations without having an agenda: boosting the acceptance of their target audience. In both cases, this is done via different approaches; in the Japanese case, with a propagandistic one, in the American case, with a counterexample. Despite all the differences, efforts, and even outcomes of those two productions, they still remain at their core what they are created for: positive representations of the armed forces.

Endnotes

1. Christopher Hughes, "The Erosion of Japan's Anti-militaristic Principles," *Adelphi Papers* 48, no. 403 (2008): 99–138, https://doi.org/10.1080/05679320902955278.
2. The narration of security threats to Japan was part of the Japanese white paper to make defense policy more intelligible to a broader audience. Manga and anime productions were just one part of the communication strategy. Japanese Ministry of Defense, *Defense of Japan* (Tokyo: Japanese Ministry of Defense, 2019), 453; and Hughes, "The Erosion of Japan's Anti-militaristic Principles," 128.
3. Takayoshi Yamamura, "Cooperation between Anime Producers and the Japan Self-Defense Force: Creating Fantasy and/or Propaganda?," *Journal of War & Culture Studies* 12, no. 1 (2019): 8–23, https://doi.org/10.1080/17526272.2017.1396077.
4. Kiyoshi Sugiyama, "Jieitai to Ōaraimachi, sonopaipuyaku to shite," in *Garupan shu zaihan*, ed. Garupan no himitsu (Tokyo: Kosaido Shinsho, 2014), 30–41. *High School Fleet*'s reception was overwhelming, even in the Western Hemisphere. A fan website for American followers was started and computer games implemented the characters in their story, with the most prominent example *World of Warships* (a free-to-play massive multiplayer online game from Belarus with an estimated 1 million players).
5. Akiko Sugawa-Shimada, "Girls with Arms and Girls as Arms in Anime: The Use of Girls for 'Soft' Militarism," in *The Routledge Companion to Gender and Japanese Culture*, ed. Jennifer Coates, Lucy Fraser, and Mark Pendleton (London: Routledge, 2019), 391–98.
6. Yamamura, "Cooperation between Anime Producers and the Japan Self-Defense Force," 17.
7. Jonathan McClory, *The Soft Power 30. A Global Ranking of Soft Power* (Portland, OR: Portland Communications, 2019); and *Testimony, Hillary Rodham Clinton, Secretary of State, Secretary of State Statement before the Senate Foreign Relations Committee*, 111th Cong. (13 January 2009) (nomination for secretary of state).
8. Yee-Kuang Heng, "Smart Power and Japan's Self-Defense Forces," *Journal of Strategic Studies* 38, no. 3 (2015): 282–308, https://doi.org/10.1080/01402390.2014.100291. An example may show the creativity of the JSDF: "MOFA cooperated with the Japan Foundation and Anime International Middle East to cover the costs of airing *Captain Tsubasa*, a popular Japanese anime cartoon series, in Iraq. *Captain Tsubasa* featured the travails of a Japanese football team and its leader. Adjusting the program for different geographical and cultural contexts, the anime screened in Iraq was dubbed in Arabic and renamed *Captain Majed*." Heng, "Smart Power," 294.
9. Sabine Frühstück, *Uneasy Warriors: Gender, Memory, and Popular Culture in the Japanese Army* (Berkeley: University of California Press, 2007); and Frühstück, "Uneasy Warriors," 117.
10. Akiko Sugawa-Shimada, "Playing with Militarism in/with *Arpeggio* and *Kantai Collection*: Effects of *shōjo* Images in War-related Contents Tourism in Japan," *Journal of War & Culture Studies* 12, no. 1 (2019): 53–66, https://doi.org/10.1080/17526272.2018.1427014.
11. Rumi Sakamoto, "Will You Go to War? Or Will You Stop Being Japanese? Nationalism and History in Kobayashi Yoshinori's Sensoron," in *China-Japan Relations in the Twenty-First Century: Creating a Future Past?*, ed. Michael Heazle and Nick Knight (Cheltenham, UK: Edward Elgar, 2008), 75–92.
12. Eric Hobsbawm and Terence Ranger, *The Invention of Tradition* (Cambridge, UK: Cambridge University Press, 2010), https://doi.org/10.1017/CBO9781107295636.
13. Paul Martin, "The Contradictions of Pop Nationalism in the Manga *Gate: Thus the JSDF Fought There!*," *Journal of Graphic Novels and Comics* 11, no. 2 (2020): 167–81, https://doi.org/10.1080/21504857.2018.1540439.
14. John A. Alic, "The Origin and Nature of the US 'Military-Industrial Complex'," *Vulcan: Journal of the Social History of Military Technology*, no. 2 (2014): 63–97, https://doi.org/10.1163/22134603-00201003.

15. Matthew Alford, *Reel Power*: *Hollywood Cinema and American Supremacy* (London: Pluto Press, 2010).
16. Sueyoung Park-Primiano, "Occupation, Diplomacy, and the Moving Image: The US Army as Cultural Interlocutor in Korea, 1945–1948," in *Cinema's Military Industrial Complex*, ed. Haidee Wasson and Lee Grieveson (Oakland: University of California Press, 2018), 227–40, https://doi.org/10.1525/9780520965263-015; and Alford, "Reel Power," 83.
17. Roberto J. González, "Introduction: Militarizing Culture," in *Militarizing Culture: Essays on the Warfare State* (New York: Left Coast Press, 2010), 13–32, https://doi.org/10.4324/9781315424699.
18. William Hamilton, "Toying with War," *Age*, 4 May 2003.
19. Alford, "Reel Power," 82.
20. Tanner Mirrlees, "Transforming Transformers into Militainment: Interrogating the DoD-Hollywood Complex," *American Journal of Economics and Sociology* 76, no. 2 (2017): 405–34, https://doi.org/10.1111/ajes.12181.
21. Kimberley Owczarski, " 'A Very Significant Chinese Component': Securing the Success of *Transformers: Age of Extinction* in China," *Journal of Popular Culture* 50, no. 3 (2017): 490–513, https://doi.org/10.1111/jpcu.12554.
22. Harlan D. Wilson, "Technomasculine Bodies and Vehicles of Desire: The Erotic Delirium of Michael Bay's Transformers," *Extrapolation* 53, no. 3 (2012): 347–64, https://doi.org/10.3828/extr.2012.19.
23. Hubert Knoblauch, Bernt Schnettler, and Jürgen Raab, "Video-Analysis: Methodological Aspects of Interpretative Audiovisual Analysis in Social Research," in *Video Analysis: Methodology and Methods. Qualitative Audiovisual Data Analysis in Sociology*, ed. Hubert Knoblauch (Frankfurt am Main, Germany: Peter Lang Verlag, 2006), 9–28, https://doi.org/10.3726/978-3-653-02667-2.
24. Knoblauch, Schnettler, and Raab, "Video Analysis," 12.
25. Hubert Knoblauch and Bernt Schnettler, "Videography: Analysing Video Data as a 'Focused' Ethnographic and Hermeneutical Exercise," *Qualitative Research* 12, no. 3 (2012): 334–56, https://doi.org/10.1177/1468794111436147.
26. Knoblauch and Schnettler, "Videography," 335.
27. The only exception is the case of Delilah, a barmaid and former assassin in the local restaurant of Alnus Hill. But even she was betrayed by Tyuule (political level) who gave her a fake order to kill a local Japanese citizen. After being stopped by the military police, she fell in love with a Japanese officer and finds a happy ending.
28. *Gate: Jieita iKanochinite, Kaku Tatakaeri (Dub)*, season 1, episode 6, "Ride of the Valkyries."
29. *Gate: Jieita iKanochinite, Kaku Tatakaeri (Dub)*, season 1, episode 8, "Japan, Beyond the Gate," Takahiko Kyōgoku.
30. Minami Funakoshi, "Foreigners in Japan Face Significant Levels of Discrimination, Survey Shows," Reuters, 31 March 2017.
31. *Transformers: Age of Extinction*, directed by Michael Bay (Hong Kong: Paramount Pictures, 2014).
32. *Transformers*.

Streaming the Battlefield
A Theory of the Internet's Effect on Negotiation Onset

First Lieutenant Anthony Patrick, USMC

Abstract: This article explores the effects of social media penetration and internet connectivity on the likelihood that parties within a conventional intrastate conflict will enter negotiations. The proliferation of advanced information communications technologies, coupled with violent political collective action, calls for further examination of how these variables intertwine to affect conflict patterns. Beginning with a discussion on communications technology and the bargaining model of war, the author presents a theoretical model that seeks to create a foundation that can be used for future empirical testing.

Keywords: negotiation onset, intrastate war, internet, communication technology

Introduction

The character of international competition has evolved significantly over the past 10–15 years. During the Cold War era, most conflicts were either intrastate wars with a hegemonic power (the United States or the Soviet Union) backing a certain side against the local proxy force for the other power. Military interventions were common during this time frame. In the aftermath of the 11 September 2001 (9/11) terrorist attacks and the fallout from the U.S.-led Global War on Terrorism, battlefield deaths from intrastate wars increased in certain parts of the globe, while other areas saw continued spillover

1stLt Anthony Patrick is currently a graduate student at the University of North Carolina Wilmington enrolled in the Conflict Management and Resolution Program. He is an active duty intelligence officer in the U. S. Marine Corps. His past work has focused on low-intensity conflict and national security policy.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201009

from the conflicts that defined the late twentieth century (e.g., Revolutionary Armed Forces of Colombia [*Fuerzas Armadas Revolucionarias de Colombia*, or FARC] in Colombia).[1]

The international playing field has begun to shift to a multipolar world, with nations such as Iran, Turkey, Russia, and China showing greater ability and willingness to participate in conflicts away from their borders either through unilateral or multilateral actions.[2] Support can be provided through financial aid, intelligence sharing, logistical support, weapons transfers, diplomatic cover for operations, and direct military intervention. Some of these conflicts have taken on aspects of earlier Cold War-era contests, with major regional powers backing opposing sides in an intrastate war.[3] These more powerful proxies are operating with foreign backing in a conventional manner, with lines of control more analogous to interstate conflict than what has been observed in conflicts such as Iraq and Afghanistan.[4]

As these conflicts have evolved during the last 10–15 years, so has the communications infrastructure used by all sides in these conflicts. Actors are more connected than ever before to local, regional, and global systems through the internet. These advanced information communications technologies (ICTs) have proliferated across the globe, with an estimated 4.6 billion internet users active today on all continents and in all countries.[5]

Pioneering scholarship within the field of ICTs and their interplay with political violence blossomed in the early 2010s, with work covering broad theories, which then narrowed down to specific empirically testable hypotheses. While these works cover a wide range of topics, a gap in the literature has been identified concerning how ICTs affect the likelihood of negotiations. Specifically, this article examines how social media penetration and internet connectivity affect the likelihood of kinetic combatants entering negotiations within a specific time frame.

Using the information-centric approach to warfare, the author will argue that the combination of social media penetration and internet connectivity helps combatants narrow the information gap that exists between them. Combating parties can monitor each other's social media accounts and independent reporters to gather information about their opponent, increasing their situational awareness. The pace of these conventional-style intrastate wars, combined with widespread access to advanced ICTs, means that the cycle of battlefield information reaching combatants is increasing exponentially. This in turn helps the combatants recognize the battlefield realities. Once each side has an accurate picture of the capabilities and limitations of the opponents, they then adjust their war goals to line up with what they could reasonably extract from the opponent at a certain cost. Once this calculation is complete, actors can then make the decision to enter negotiations faster than what has been the historic norm.

This research can assist policy makers in two main ways. First, it can assist conflict forecasters in understanding what factors may influence the progression of a conflict. If they can obtain a solid grasp of the information space that combatants are operating in, they can begin to better understand why combatants are taking a certain course of action within the conflict. Second, knowing how information flow affects negotiation onset could aid conflict managers in identifying low-cost interventions that could shorten conflict duration. These interventions, coupled with additional methodologies, could help reduce the cost of conflict, both in terms of financial cost and lives lost.

This article establishes a theoretical analysis of the effects of ICTs on the likelihood of negotiation onset within the context of interstate wars that take on conventional characteristics. Next, the information-centric approach to warfare will be discussed in depth. In the fourth section, the author will introduce the bargaining model of war. Taking all this information into account, the author will then introduce an explanatory theory of how advanced ICTs affect the likelihood of negotiations.

ICTs' Effect on Armed Conflict

The last two centuries has seen a rapid growth in humanities' ability to quickly communicate larger volumes of information across ever-increasing distances. The introduction of the telegraph made it possible for people to quickly pass messages across the Atlantic, drastically reducing the time for a recipient to get a message. The telephone made instant voice point-to-point communications possible, redefining how groups within society interact. The post–World War I years saw political movements, cultural icons, and companies expand their reach with the introduction of the radio, creating for the first time in human history readily available point to mass communication systems. During World War II, millions of citizens received battlefield updates through easy access to film, which expanded further in the postwar era with the widespread introduction of television.

While this growth is substantial, it pales in comparison to the growth in information sharing the world has experienced in the last 30 years. The combination of cell phone technology, social media, and the internet has made it possible for point-to-point *and* point-to-mass communications of large volumes of information from almost anywhere in the world. Both endogenous and exogenous connections have in many ways brought aspects of the human experience to our fingertips.

A large body of research demonstrates the connection between ICTs and collective action. Linkages formed by ICTs reduce the cost for mobilization.[6] This is in line with theories proposed by other scholars, pointing out that a central determinant to collective action is the mobilization cost imposed on leaders.[7] ICTs help a group by allowing it to exchange a greater volume of information with more of its members over a shorter period of time. Amplifying this effect is the disaggregated nature of modern-day ICTs. Wireless devices make it possible for decentralized groups to quickly mobilize en masse.

There are numerous examples of ICTs being used for political collective action in various localities across the globe. Social media has been used to mobilize protesters in Russia, with the most significant effects being observed in areas where one social media site holds a monopoly over local accounts.[8] At the time of writing, Nexta, a social media channel in Belarus, is using WhatsApp to organize weekend protests against the Belarusian government from Poland, mobilizing tens of thousands and directing them to specific government-owned properties from hundreds of miles away.[9]

This mobilization can also be used toward violent collective action, which is a subset of political collective action. Various studies have examined the relationship between violence and the proliferation of ICTs, demonstrating both positive and negative effects.[10] In their flagship work within the field, Jan H. Pierskalla and Florian M. Hollenback demonstrate empirically that cell phone coverage increases violent activity within the context of intrastate violence.[11] The cycle of violence is expedited through the use of instant communication through ICTs to disaggregated networks, allowing actors to communicate directives to specific targets faster than ever before.[12] This trend is further observed by the work of Catie Snow Bailard, who narrows down the unit of analysis to focus on violent collective action between specific ethnic groups.[13] The author shows (with an expanded data set) that the introduction of mobile cell technology increases the probability that groups will engage in conflict with their government. A unique finding by Bailard shows that this effect is dampened in regions with increased access to landline communications. Municipalities that have robust landline access already have the ability (albeit not mobile) for point-to-point communication. Thus, the introduction of cell phone access does not change a citizen's ability to communicate directly with others within their community. A community that relies solely on radio communication (point to mass) will see a greater effect from the introduction of cell phones than one that relies more on landline connectivity. This implies that the true increase comes from the shift to instant mobile point-to-point communication through cell phones and internet access and not just the introduction of point-to-point communication.

Cellular communications through 3G and 4G technologies allow users to access the internet and thus social media platforms. The evolution of social media is one of the most unique advances in how we communicate. While the radio introduced point to mass communication and the phone perfected point-to-point communication, social media allows a user to communicate both vertically and horizontally throughout society. Sites like Twitter and Facebook allow a user to share information within a closed group of followers or friends (horizontal) who can then instantly take that information and share it with out-of-group members who were not directly connected to the initial user (vertical). This expands both the number of nodes within a system an individual can influence as well as the speed of which that influence can spread.

Since this communication can originate from the masses, it challenges the historic control political elites have had on the information sphere. The use of segmented and encrypted networks creates a more diverse information environment, especially in communities where the central authorities lack enforcement mechanisms.[14] These segmented networks push the internet to become increasingly endogenous to the local context.[15] Initial inroads into the effects of social media on violent collective action show that social media penetration generates substantial increases in violent collective action, especially in areas that lacked mass communication technologies prior to the introduction of social media.[16] It is important to note that these effects are observed in areas where a history of armed conflict exists. The introduction of new communications does not mean a stable political situation will inherently descend into violence (think adding 5G technology into countries such as the United States and Germany).

The above work has established a baseline for ICTs' effect on violent collective action, but there are some limitations of the literature. These works might lead one to suspect that the number of peaceful and violent movements have increased with the introduction of advanced ICTs. Instead, it is the number of events within each conflict that has increased, not the number of conflicts, thus demonstrating the dichotomy between the macro and micro effects of ICTs.[17] While the lack of data on rural cellular access might limit the findings of certain empirical studies, the various investigations in the field show strong evidence that ICTs can be used to increase violent collective action by reducing the cost of communication, increasing the volume of information shared, and massing disaggregated group members in an expedited manner.[18]

These studies have a few key implications. First, advances in ICTs can affect both political collective action and violent collective action. Groups can decide how to use ICTs to accomplish their objectives. Larger volumes of information can be shared to more nodes who are geographically disaggregated at a lower cost and within a shorter period. Second, the greatest effect on violent collective action can be observed in cases where an advancement in ICTs changes the *nature* of how nodes within a system communicate. Studies have demonstrated that increasing data rates (i.e., 3G to 4G) do not lead to a statistically significant increase in violence.

Data rates can be conceptualized as changes in the character of communications as it might change different sites or data types that are transmitted. For example, moving from 3G to 4G means that users can post higher quality videos on social media sites. Videos with more detail transmit more information, which can be a change in the character of communication. However, moving from 3G to 4G does not make an individual use an inherently different system for communication, which would be a change in the *nature* of communication. They are still using the same, if maybe an updated version, of the social media site. Changes in the *nature* of communication are more indicative of evolutions that rearrange in a systematic way how nodes within a system are connected. Finally, advances in ICTs disproportionally benefit nonstate actors when compared to state actors. This is because before the proliferation of these technologies, most states have maintained a working communications system between nodes within the state, having the resources to invest in phone lines and military-style radio communications. These methodologies have historically been price prohibitive for nonstate actors. Cheap and effective ICTs have significantly closed this gap. When combined, these three findings indicate that advances in ICTs have a direct effect on how nodes within a system interact and thus will also affect the cycle of violent collective action experienced by these groups.

Information-centric Approach to Warfare

Information has always been a vital component of warfare. Yet, it has historically not been viewed as equivalent to other determinants of war outcomes. Early work on the concept of "netwar" focused on how insurgents, criminals, and social activists will use the growing information environment as its own conflict space.[19] Factors such as natural resources, economic power, and military strength have been used by many to examine war outcomes of conflicts. However, information is an equally important component in the execution of war. The work of Eli Berman, Joseph H. Felter, and Jacob N. Shapiro is a notable empirical work that emphasizes the role of information in contemporary conflicts.[20] The study introduces an information-centric approach to warfare, which they derive from their experience supporting operations in both Iraq and Afghanistan. One key insight of the study is that asymmetric conflicts like the complex intrastate conflicts described in the first section are inherently information-centric. In other words, the information environment is a key space of contestation between the conflicting parties. Each of the contending belligerent parties is trying to outmaneuver the other within the information realm to gain an advantage over the other.

Within an information-centric conflict, the key factor is the flow of information. Economic or military capacity at the macro level will not have a substantive effect on the conflict outcome if the flow of information remains constant or is advantageous to an adversary at the local level.[21] For this flow to be effective, it must be consistent and digestible by the intended audience. This approach is more relevant to the complex intrastate conflicts today, since battles are smaller in scale and local-level factors have a greater impact on the outcomes.[22] As mentioned in the second section, access to advanced ICTs has direct consequence to the information-centric battlespace.

The amount of data being produced in the global south has grown at an exponential rate from the mid-2000s to the late 2010s.[23] For example, India is creating the digital infrastructure to provide all of its 1.2 billion residents with a unique online identification. Myanmar, a country rife with internal violent conflicts, experienced a 50-fold increase in internet users from 2007 to 2014. Providers within the information space are therefore diverse not only in their numbers but also in the services they can provide. Even in conflict-torn Syria, a total of nine internet service providers *expanded* service by 1.6 million users between 2010 and 2016, demonstrating growth in a nation embroiled in a civil war. While this list is in no way exhaustive, it demonstrates that historically underdeveloped parts of the world are quickly experiencing a rapid increase in the availability of internet access. With the right penetration of internet connectivity and social media access, internal conflicts will be fought in the kinetic battle space as well as the information realm. This makes the information-centric approach to warfare applicable with the flow of information potentially being a key determinant of battlefield outcomes and how those outcomes are communicated to decision makers on both sides of the trenches. Before an examination of how the information-centric approach to war interplays with the likelihood of conflicting parties entering negotiations, it is important to understand the bargaining model of war.

Bargaining Model of War

Wars generally start when one group believes they have the necessary strength to extract concessions from another group through force. These demands can be for either territory, natural resources, political subjugation, or cultural differences. No matter what the nature of the dispute, war equates to groups using violent means against another group to change the status quo between them. This also means that war is an interaction between groups. It is through this violent interaction that groups begin to discover more about their opponent. Whether it be their relative strengths or the resolve to fight, battles expose information about a group's opponent. Examining wars from this bargaining model helps us understand how information flow is vital to outcomes like negotiated settlements.

Dan Reiter's work into the bargaining model of war lays out a comprehensive understanding of how this interaction plays out in armed conflict.[24] The main problem actors face is that they cannot all achieve their most desired goals simultaneously due to scarcity. This can be due to limited physical resources (e.g., oil), trying to maximize political support within a nation, or alignment of different leaders within a religious framework. The *bargaining model* sees the essence of conflict as a disagreement over resource allocation or policy choice. Thus, war happens because sides disagree about their ability to inflict unsustainable costs on their opponent while simultaneously absorbing costs imposed on themselves by the opponent to settle that disagreement over resource allocation. These wars emerge from the perceptual biases and miscalculations of each actor, who build their cost-benefit analysis based on their framing of the problem. This means that what might be costly to one actor is not a concern for another (i.e., cultural/religious differences). Interactions (kinetic and nonkinetic) between the adversaries reveals information about each other, causing expectations of the two sides to converge and opening up space for negotiation onset.

The work of Darren Filson and Suzanne Werner provides a more in-depth description of kinetic actions within the bargaining model of war. Using a causal chain of analysis, the authors argue that in a perceived equilibrium, an attacker never provokes a fight with a defender since the benefits of such adventurism tends to outweigh the costs.[25] Wars only begin when the attacker believes they have an advantage over the defender and that they have the means to exploit those gaps. The attacker's private information about their chances of winning battles evolves in response to a defender's rejections of the attacker's demands. The defender's rejection is in turn informed by battlefield results and their own internal cost-benefit analysis of continuing to fight. This means that the private information about their own capability and their (one-sided) belief about their relative strength informs their next move. The revelation of mutual strength can reduce uncertainty, thus shortening war duration.[26]

Further work in the field has empirically reinforced the bargaining model of war presented by Filson and Werner. Information about relative military strength is a key driver during the mediation process, with intrastate conflicts between groups being the most likely to enter negotiations when they are at parity than groups with greater power asymmetry.[27] Additionally, the location of battles also plays an important role in the calculus of parties. States are less likely to enter negotiations when the rebels are at the gates of the capital as the government knows that it is in a significantly weaker negotiating position.[28] This was seen in the Libyan Civil War (2011–20), where the Government of National Accord (GNA) and Libyan National Army refused negotiations while Tripoli was under siege. It was not until the GNA's quick succession of battlefield victories in early fall of 2020 that the sides agreed to enter into more substantial talks.

A leader's information concerning the population's willingness to continue fighting also impacts the duration of conflict. Research suggests that war weariness among the masses increases willingness for sides to enter negotiations.[29] A common thread in all these critical group decisions to continue the war is the information environment. The murkier the waters, the harder it is for groups to resolve their uncertainty of the situation. Previous work has demonstrated that negotiations are less likely to happen when multiple actors join the fold, adding more uncertainty to the strategic calculations.[30] While there are strong incentives for parties to misrepresent information (e.g., through misinformation campaigns) as long as that information is believed by the targeted party, it will still be used by them to shape their understanding of the battlespace.[31] The bargaining model of war provides key insights into the factors that influence when parties will enter negotiations with their adversary. What is needed is a theoretical approach that combines the bargaining model of war presented by Filson and Werner with the new information environment that groups operate within during modern intrastate conflicts.

Social Media and Likelihood of Negotiations

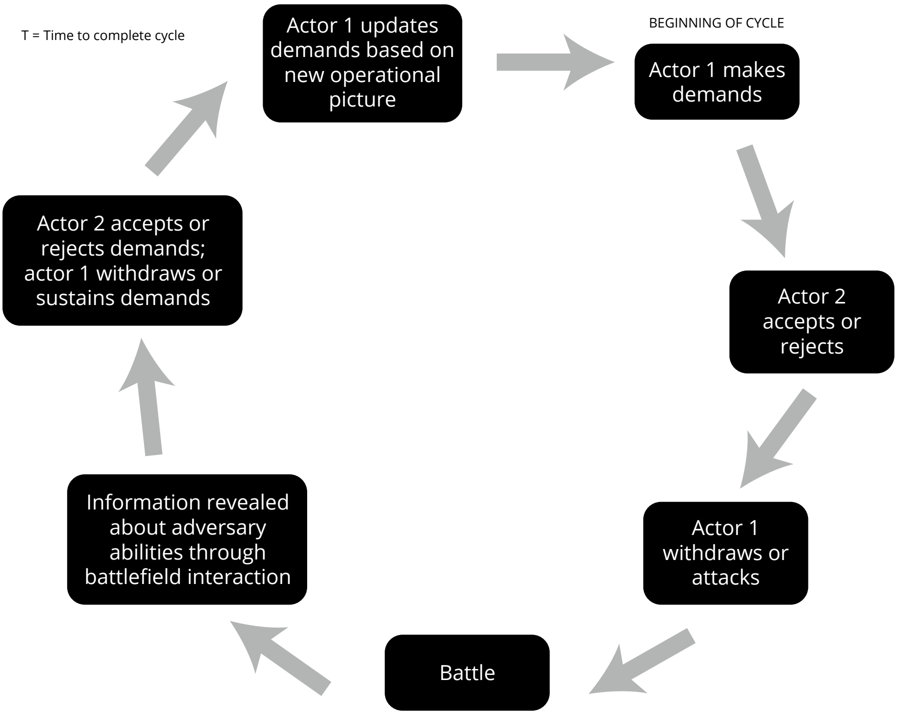
Taking into account the discussion above, the author examined how social media and internet connectivity affects war decision making. This model is not meant to be universal in nature. The effects of social media penetration and internet connectivity vary depending on the type of conflict the actors are involved in. This model focuses on intrastate wars where the conflict takes on conventional characteristics and neither side has robust intelligence agencies. This is because actors with robust intelligence agencies would not rely on open-source reporting for the majority of their information. The model focuses on information instead of intelligence, since intelligence is information that has been evaluated, analyzed, and synthesized into a certain context.[32] The conflict also needs to be conventional in nature, where both sides can control territory and deny the adversary access to that territory. This is important because the bargaining model of war breaks down once you move into conflicts where parties do not have some level of parity. Without near parity there is no true incentive for the powerful party to enter negotiations with the significantly weaker power.

Additionally, this model focuses on intrastate wars because in most of these conflicts the actors have the funds to sustain the above-mentioned intelligence capabilities. Actors are incentivized to use the internet and social media for a variety of reasons. First, it is the most immediate feed of information from all sides within a conflict. Groups will use it to monitor social media accounts of the opponents to try to gather exploitable information, which they can do easily since the service is inexpensive and mobile. This is negated when one state actor is able to impose a communications blackout on a region, similar to what has occurred in the 2020 Ethiopian-Tigray conflict.[33] However, in some countries, control of the communications infrastructure is not as centralized, making it difficult for one side to institute a large-scale information blackout. Second, the internet and social media combine quick feedback of information that originates from multiple nodes in the system, thus providing an avenue to confirm information received from one source.[34] It is important to keep in mind that this model does not take into account the effects of misinformation. This model is not focused on the flow of factually correct information. Instead, it focuses on the flow of information that can shift the mindset of influencers within each respective actors' system. As long as the actor believes the information to be true, that information will influence the actor's decision-making cycle.

Wars are a constant revolving interaction between actors. With this in mind, the following model can be deduced, explaining the interaction between the likelihood of negotiation onset, social media penetration, and internet connectivity. First, actor 1 uses the information they already have on actor 2's (the adversary) capabilities and limitations. Using that information, they make a demand of actor 2. Actor 2 then either has the option to give in to actor 1's demands or to deny them. If actor 2 gives in, the cycle is broken and the interaction ends. If actor 2 denies the demands, actor 1 has the option to either back out (maintaining the status quo) or to attack actor 2 to force them to capitulate. The two sides then take their dispute to the battlefield, where a complex series of variables clash violently with the outcome being unpredictable.

During the battle, both actors learn more about the capabilities and limitations of their adversary based on their battlefield performance. After the battle has concluded, both actors face another decision point. Actor 2 can either give in to the original demands of actor 1 or continue resistance. Actor 1 can either withdrawal their demands or continue with the same demands. If actor 2 continues resistance and actor 1 does not withdraw, then the cycle repeats with actor 1 making demands of actor 2. This cycle takes a certain amount of time (T), which varies based on battle duration, the initial interactions over demands, and how long it takes actors 1 and 2 to respond to the results of the battle. With an updated picture of the adversary's abilities, revealed through battle, actor 1 can either sustain their current demands or adjust them based on the new operational picture. At each point in the cycle, either actor 1 or 2 can decide to enter negotiations, trying to reach a middle ground between actor 1's demands and actor 2's rejection of any concessions. As the conflict continues, this cycle is repeated, and the actors get closer to reaching information certainty. It is important to note that neither actor can ever reach true information certainty, as the chaotic nature of war always leaves information unknown to both

Figure 1. Bargaining model cycle

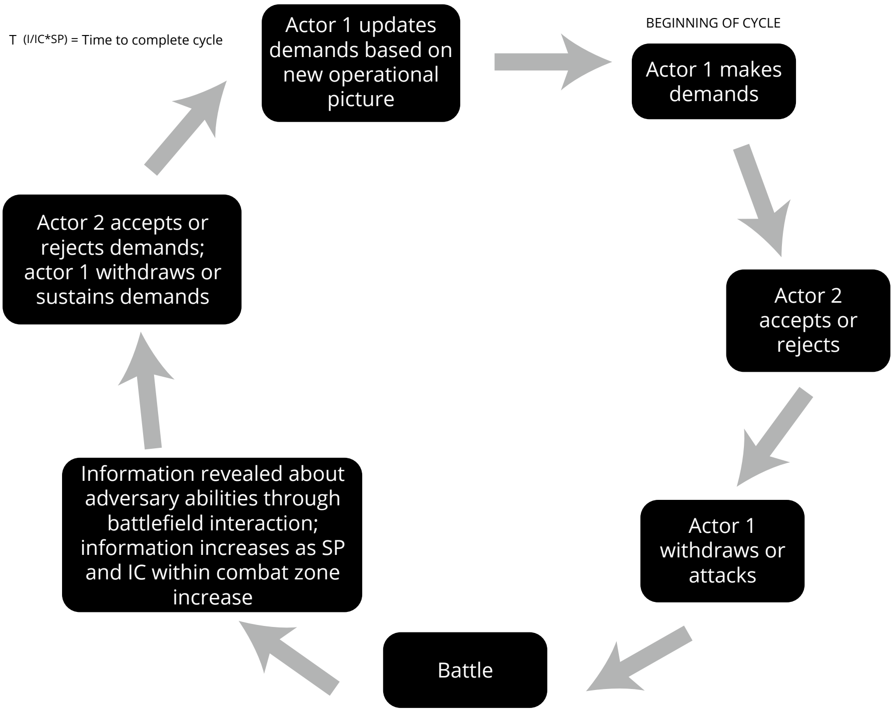

T = Time to complete cycle
Actor 1 updates demands based on new operational picture
BEGINNING OF CYCLE
Actor 1 makes demands
Actor 2 accepts or rejects demands; actor 1 withdraws or sustains demands
Actor 2 accepts or rejects
Information revealed about adversary abilities through battlefield interaction
Actor 1 withdraws or attacks
Battle

Source: Courtesy of author, adapted by MCUP.

actors. However, the closer the actors get toward this level of perfect knowledge, the better informed their decision-making process will become. Greater information certainty will allow each actor to understand what end state they can likely achieve based on the power dynamics between them. If both actors conclude that complete victory is unlikely, they will attempt to enter negotiations with their adversary. This will be required to obtain their most desired end state within the conflict since neither side can force all of their demands on their adversary.

Figure 1 depicts how the bargaining model of war can operate as a cycle, with battles revealing information that forces leaders to reevaluate their decision making. Modern intrastate wars that take on conventional characteristics operate in a similar manner. However, the introduction of social media penetration (SP) and internet connectivity (IC) expedite this process. The first half of figure 2 remains the same. Where SP and IC start to influence the system is after the battle. The combined effect of SP and IC increases the value of the perception of the adversary's capabilities and limitations. Various nodes in an interconnected information system reveal more information to actor 1 and actor 2 and provide verification mechanisms that strengthen those perceptions of the adversary's capabilities and limitations. Additionally, since SP and IC allow actors 1

Figure 2. Impacts of internet connectivity and social media penetration on the bargaining model cycle


T (I/IC*SP) = Time to complete cycle
Actor 1 updates demands based on new operational picture
BEGINNING OF CYCLE
Actor 1 makes demands
Actor 2 accepts or rejects
Actor 1 withdraws or attacks
Battle
Information revealed about adversary abilities through battlefield interaction; information increases as SP and IC within combat zone increase
Actor 2 accepts or rejects demands; actor 1 withdraws or sustains demands

Source: Courtesy of author, adapted by MCUP.

and 2 to obtain clearer pictures of the true capabilities and limitations of their adversary, they hasten the decision-making cycle of actors 1 and 2 and reduce the time it takes for each cycle to complete. Since actors 1 and 2 can complete more cycles in a shorter period of time, it theoretically increases the likelihood that actors 1 and 2 will enter negotiations within a given time frame since it closes the information gap between both sides and limits uncertainty.

After running through this model, there are two hypotheses that can be tested in future empirical work:

> ***H1:*** *Higher levels of social media penetration and internet connectivity increase the likelihood that conflicting parties will enter negotiations.*
>
> ***H2:*** *The effects of social media access on the likelihood of a dyad entering negotiations decreases over time as the number of active rebel groups in a conflict zone increases.*

H1 focuses on the main topic of this article. H2 expands on H1 by taking into account complex conflicts where multiple disaggregate parties battle each other in a conventional style (e.g., the Syrian Civil War [2011–present], First Congo War [1996–97], and the Libyan Civil War). While more actors within the system increase the flow of information, the myriad of sources and competing dyads muddies the information waters, thus reducing the effects of SP and IC. H1 was selected because it is the most directly testable hypothesis pulled from the aforementioned model. H2 was selected to allow for an additional testable hypothesis that specifically takes into account multifaceted intrastate conflict. These hypotheses provide a baseline for future empirical testing.

Conclusion

The introduction of new communications technologies has altered the way humans interact. Violent political collective action has also been affected by these advances. Understanding how these technologies affect intrastate wars can have important policy implications. For example, nongovernmental organizations may change the way they interact with parties within a conflicting dyad. If they know that social media access helps the sides enter negotiations faster, they may try to invest in reporting methodologies to decrease decision-maker uncertainty within the information space. For government agencies, knowing which information sources influence decision makers within a conflicting dyad can give the government another avenue to push parties toward maintaining the status quo or entering negotiations before a war even starts by reducing decision-maker uncertainty. The gathering, analysis, and spread of information is a vital part of modern-day conflict.

This article aimed to lay out an explanatory model for how social media penetration and internet connectivity can increase the likelihood of actors entering negotiations by reducing the amount of time it takes for both actors to close their information gaps. The next step in the research process is to test this model empirically. Expected challenges involve measuring internet connectivity, measuring social media penetration, defining intrastate conventional conflicts with quantitative measures, controlling for confounding variables, and defining negotiation onset. A better understanding of how the evolving communications landscape interplays with intrastate conflict is important to inform policy makers on how best to allocate resources toward certain lines of effort.

Endnotes

1. "FARC," Uppsala Conflict Data Program, accessed 8 February 2021; and Alexandre Marc, *Conflict and Violence in the 21st Century: Current Trends as Observed in Empirical Research and Statistics* (Washington, DC: World Bank Group, 2015).
2. Timothy R. Heath, *China's Pursuit of Overseas Security* (Santa Monica, CA: Rand, 2018), https://doi.org/10.7249/RR2271; Nakissa Jahanbani, "Reviewing Iran's Proxies by Region: A Look Toward the Middle East, South Asia, and Africa," *CTC Sentinel*

13, no. 5 (May 2020); and Candace Rondeux and David Sterman, *Twenty-First Century Proxy Warfare: Confronting Strategic Innovation in a Multipolar World* (Washington, DC: New America, 2019).

3. Maj Amos C. Fox, USA, *In Pursuit of a General Theory of Proxy Warfare*, Land Warfare Paper 123 (Arlington, VA: Institute of Land Warfare, 2019).
4. "Syria Situation Report: January 8–29, 2021," understandingwar.org, 29 January 2021; and Alia Chughtai and Ramy Allahoum, "Libya: Mapping Areas of Military Control," Al Jazeera, 27 July 2020.
5. "Worldwide Digital Population as of October 2020," Statista, 27 January 2021.
6. Anita Breuer, Todd Landman, and Dorothea Farquhar, "Social Media and Protest Mobilization: Evidence from the Tunisian Revolution," *Democratization* 22, no. 4 (2015): 764–92, https://doi.org/10.1080/13510347.2014.885505.
7. Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, MA: Harvard University Press, 1965).
8. Ruben Enikolopov, Alexey Makarin, and Maria Petrova, "Social Media and Protest Participation: Evidence from Russia," *Econometrica* 88, no. 4 (2020): 1479–1514, https://doi.org/10.3982/ECTA14281.
9. George Barros, "Warning: Kremlin-linked Belarusian Opposition Leadership Threaten to Further Fragment Opposition Unit," Institute for the Study of War, 1 September 2020; and Zachary C. Steinert-Threlkeld et al., "Online Social Networks and Offline Protest," *EPJ Data Science* 4, no. 19 (2015): 4–19, https://doi.org/10.1140/epjds/s13688-015-0056-y.
10. T. Camber Warren, "Not by the Sword Alone: Soft Power, Mass Media, and the Production of State Sovereignty," *International Organization* 68, no. 1 (2014): 111–41, https://doi.org/https://doi.org/10.1017/S0020818313000350; and David Yanagizawa-Drott, "Propaganda and Conflict: Theory and Evidence from the Rwandan Genocide" (working paper, Center for International Development at Harvard University, Cambridge, MA, 2012).
11. Jan H. Pierskalla, and Florian M. Hollenbach, "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa," *American Political Science Review* 107, no. 2 (May 2013): 207–24, https://doi.org/10.1017/S0003055413000075.
12. It is important to note that ICTs do not begin this cycle as there are many other conditions that interplay during conflict onset. Ted Gurr, "Psychological Factors in Civil Violence," *World Politics* 20, no. 2 (January 1968): 245–78, https://doi.org/10.2307/2009798, provides a good look into the psychology of conflict onset.
13. Catie Snow Bailard, "Ethnic Conflict Goes Mobile: Mobile Technology's Effect on Opportunities and Motivations for Violent Collective Action," *Journal of Peace Research* 52, no. 2 (2015): 323–37, https://doi.org/10.1177/0022343314556334.
14. Thomas Zeitzoff, "How Social Media Is Changing Conflict," *Journal of Conflict Resolution* 1, no. 22 (2017), https://doi.org/10.1177/0022002717721392.
15. Anita R. Gohdes, "Studying the Internet and Violent Conflict," *Conflict Management and Peace Science* 35, no. 1 (2018): 89–106, https://doi.org/10.1177/0738894217733878.
16. T. Camber Warren, "Explosive Connections?: Mass Media, Social Media, and the Geography of Collective Violence in African States," *Journal of Peace Research* 52, no. 3 (2015): 297–311, https://doi.org/10.1177/0022343314558102.
17. Erica Chenoweth and Maria Stephan, *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict* (New York: Columbia University Press, 2011).
18. Allan Dafoe and Jason Lyall, "From Cell Phones to Conflict?: Reflections on the Emerging ITC Political Conflict Research Agenda," *Journal of Peace Research* 52, no. 3 (May 2015): 401–13, https://dx.doi.org/10.2139/ssrn.2409639.
19. John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: Rand, 2001), https://doi.org/10.7249/MR1382. Netwar was first defined by Rand as a "societal conflict and crime, short of war, in which the antagonists are organized more as sprawling 'leaderless' networks than as tight-knit hierarchies."

20. Eli Berman, Joseph H. Felter, and Jacob N. Shapiro, *Small Wars, Big Data: The Information Revolution in Modern Conflict* (Princeton, NJ: Princeton University Press, 2018).
21. Berman, Felter, and Shapiro, *Small Wars, Big Data*.
22. Lotta Themnér and Peter Wallensteen, "Armed Conflicts, 1946–2013," *Journal of Peace Research* 51, no. 4 (2014): 541–54, https://doi.org/10.1177/0022343314542076. Note: the observance of lower battle being smaller in scale is due to the observed increase in armed intrastate conflicts that corresponds with an observed decrease in battle-related fatalities, meaning that less people are dying in an expanding series of armed conflicts.
23. Paya Arora, "The Bottom of the Data Pyramid: Big Data and the Global South," *International Journal of Communication*, no. 10 (2016): 1681–99.
24. Dan Reiter, "Exploring the Bargaining Model of War," *Perspectives on Politics* 1, no. 1 (March 2003): 27–43, https://doi.org/10.1017/S1537592703000033.
25. Darren Filson and Suzanne Werner, "A Bargaining Model of War and Peace: Anticipating the Onset, Duration, and Outcome of War," *American Journal of Political Science* 46, no. 4 (October 2002): 819–37, https://doi.org/10.2307/3088436.
26. Govinda Clayton, "Relative Rebel Strength and the Onset and Outcome of Civil War Mediation," *Journal of Peace Research* 50, no. 5 (2013): 609–22, https://doi.org/10.1177/0022343313491587.
27. Philip Hultquist, "Power, Parity, and Peace?: The Role of Relative Power in Civil War Settlement," *Journal of Peace Research* 50, no. 5 (2013): 623–34, https://doi.org/10.1177/0022343313486281; J. Michael Greig, "Nipping Them in the Bud: The Onset of Mediation in Low-Intensity Civil Conflicts," *Journal of Conflict Resolution* 59, no. 2 (2015): 336–61, https://doi.org/10.1177/0022002713503807; and David E. Cunningham, Kristian Skrede Gleditsch, and Idean Salehyan, "It Takes Two: A Dyadic Analysis of Civil War Duration and Outcome," *Journal of Conflict Resolution* 53, no. 4 (2009): 570–97, https://doi.org/10.1177/0022002709336458.
28. Sema Hande Ogutcu-Fu, "Outside the Battlefield: In-Group Political Dynamics of Civil Conflict Negotiations and Settlements," *Political Science Quarterly* 69, no. 3 (2016): 403–17, https://doi.org/10.1177/1065912916648010.
29. David E. Cunningham, "Veto Players and Civil War Duration," *American Journal of Political Science* 50, no. 4 (October 2006): 875–92, https://doi.org/10.1111/j.1540-5907.2006.00221.x.
30. Desiree Nilsson, "Turning Weakness into Strength: Military Capabilities Multiple Rebel Groups and Negotiated Settlements," *Conflict Management and Peace Science* 27, no. 3 (2010): 253–71, https://doi.org/10.1177/0738894210366512.
31. Dafoe and Lyall, "From Cell Phones to Conflict?," 401–13.
32. *Intelligence*, Marine Corps Doctrinal Publication 2 (Washington, DC: Headquarters Marine Corps, 2018). Recent scholarship has found a statistically insignificant relationship between external provision of intelligence and conflict termination. See Katherine Sawyer, Kathleen G. Cunningham, and William Reed, "The Role of External Support in Civil War Termination," *Journal of Conflict Resolution* 6, no. 61 (2017): 1174–1202, https://doi.org/10.1177/0022002715600761.
33. Following a disputed federal and regional elections process in the summer and fall of 2020, the Ethiopian government and regional government of Tigray opened kinetic hostilities with each other. On 4 November, the Ethiopian government blocked out the majority of communications within the region, making it incredibly difficult for outsiders to get information on troop movements and battlefield results.
34. Bailard, "Ethnic Conflict Goes Mobile," 323–37. This theory at first glance appears to be in contention with the work of Bailard, whose findings indicate that an increase in cell service increased the probability of violent conflict between rebels and the government. However, this theory examines how social media penetration and internet connectivity affect the likelihood of negotiation onset. The same technology that groups use to mobilize supports before and during conflict onset can also be used for information collection (as examined earlier).

The Crucible of War
What Do We Know about Military Adaptation?

Martijn van der Vorm

Adaptation under Fire: How Militaries Change in Wartime. By David Barno and Nora Bensahel. New York: Oxford University Press, 2020. Pp. 440. $34.95 (hardcover). https://doi.org/10.1093/oso/9780190672058.001.0001.

Learning the Lessons of Modern War. Edited by Thomas G. Mahnken. Stanford, CA: Stanford University Press, 2020. Pp. 336. $105.00 (hardcover); $35.00 (paperback).

Introduction

How military organizations acquire and implement new knowledge, both in and out of conflict, has been subject to intense study during the last few decades. This academic subfield is known as military innovation studies.[1] In the last 15 years, this subject has gained even more prominence. In large part, this can be ascribed to the extensive scholarly work concerning the experiences of Western armed forces during their deployments in Iraq and Afghanistan.[2]

In war, militaries will seek to adapt to operational challenges to gain an edge over the enemy. Moreover, as the adversary learns simultaneously, learning and adapting during war is considered critical to stave off defeat and even to ensure survival.[3] Evidently, military planners will also seek an advantage prior to war.

Martijn van der Vorm is an officer (major) at the Royal Netherlands Army. He has been deployed on multiple tours to Afghanistan and the Middle East. Currently, he is pursuing a PhD at the Netherlands Defence Academy, The Hague. His research focuses on learning and institutionalization processes by Western armed forces in relation to irregular warfare. Martijn holds MAs in history and military strategic studies.

Solutions to a hypothetical operational challenge can manifest in implementing new technologies, trying out new concepts, introducing new competencies, and allocating additional resources or a combination of those elements.[4] Accordingly, military innovation studies encompass both adaptation and innovation. The distinction between these two terms has been the subject of academic debate.[5] Theo Farrell posits that adaptation and innovation are part of a continuum. In his view, adaptation indicates adjustments while innovation "implies a greater degree of novelty and disruptive organizational change."[6]

Another distinction is made by Williamson Murray based on the dissimilar circumstances of war and peace. According to Murray, adaptation occurs during wartime as militaries grapple with the pressures of the enemy's activities and the operational environment created by them. Innovation is exclusive to peace as military organizations have time to think through the implications of change but lack the practical feedback that war provides.[7] In a general sense then, military innovation studies can be divided into three broad categories: the introduction of novel technologies and concepts in peacetime, adaptation to operational challenges in wartime, and institutionalization of lessons from previous conflicts.[8] Still, it is important to note that resolving identified deficiencies in military organizations and operations do not necessarily lead to enhanced performance, let alone results. As the enemy invariably adapts as well, its actions can negate any beneficial effects of adaptations. Furthermore, the innumerable manifestations of friction in the operational environment can diminish the results of organizational improvements.[9] In the case of the wars in Iraq and Afghanistan, all the identified adaptations did little to further a satisfactory strategic outcome.

Recently, two interesting books were added to the firmament of military innovation studies: *Adaptation under Fire: How Militaries Change in Wartime* by David Barno and Nora Bensahel and *Learning the Lessons of Modern War* edited by Thomas G. Mahnken. The new publications chronicle the adaptations and lessons for the United States and its allies in Iraq and Afghanistan. Additionally, *Learning the Lessons of Modern War* examines other recent conflicts, such as those in Sri Lanka, Colombia, Georgia, and the Philippines. Both works describe wartime adaptation. To a lesser extent, Mahnken's edited volume considers the utility of lessons from recent wars for future conflict.

The two new books take different approaches to examining adaptations. *Adaptation under Fire* tries to find causal mechanisms to provide general explanations for the phenomenon of military adaptation. From such inquiries, scholars and policy makers can potentially draw prescriptions that can ameliorate practical deficiencies.[10] The objective of the book is to examine the adaptability of the U.S. military for future war by taking stock of its recent experiences in Afghanistan and Iraq.[11] Furthermore, it seeks to offer recommendations to improve adaptability in the U.S. military. Conversely, Mahnken's edited volume takes a historical approach by describing various recent case studies. As such, it is light on theory but rather seeks to study recent history to understand "continuity and change in the character and conduct of war."[12]

This review essay will consider the contribution of these works to the field of military innovation studies. To this end, this essay is divided in three parts. First, the salient developments, tenets, and debates of military innovation studies are examined. The second part aims to gauge the merit of the new books by Barno, Bensahel, and Mahnken and how they can be positioned in the literature. Finally, the third part will briefly discuss the current state of the literature and potential directions for additional research.

Military Innovation Studies: Developments and Challenges

Widely regarded as the founder of military innovation studies, Barry R. Posen emphasized peacetime innovation in new doctrinal concepts that integrated new technologies in the interwar period. He contended that military organizations are inherently resistant to change and therefore require civilian intervention to force new concepts upon them.[13] Another influential early author, Stephen Rosen, recognized that armed forces adapt to wartime challenges. However, he regarded these changes as less sweeping and effective due to the constraints imposed by operational pressures. Rosen argued that during wartime, militaries lacked the time and necessary information to introduce novel concepts and technologies that fall outside of the normal framework of their mission.[14] Instead, more profound innovations are driven by competition between branches within a Service in a search toward "a new theory of victory."[15] An early example of how armed forces learned from previous wartime experiences is the work of Richard Duncan Downie. He studied the extent to which the U.S. military incorporated its experiences in irregular warfare in its doctrine. For his research, Downie employed organizational learning theory, which studies how organizations learn from interactions with their environment and subsequently seek to enhance their performance.[16] He found that organizational change comes from alignment of external factors, such as enemy actions, with internal ability and willingness to learn from external events.[17]

Thus, the early literature on military innovation illustrated a broad array of potential explanations for how and why armed forces change to existing or potential external challenges and organizational deficiencies. In 2006, Adam Grissom took stock of the field in an influential article, "The Future of Military Innovation Studies." He categorized the various explanations for military innovations offered up to that point in four schools of thought: civil-military relations, inter-Service rivalry, intra-Service rivalry, and cultural factors.[18] More important than this categorization itself, Grissom concluded that the four schools of thought were generally in accordance that military organizations are inherently averse to change. As a result, change in military organizations was regarded as process that is initiated from the top down.[19] Yet, this vantage point ignored historical evidence that suggested that significant innovations (or adaptations) were initiated by troops in the field during operations. To remedy this academic lacuna, Grissom called for both more intensive empirical study into bottom-up innovation and establishing new conceptual models that identify the necessary conditions for this grassroots innovation to occur.[20] Interestingly, Grissom explicitly discounted literature on organizational learning as a conceptual model. Although this had been used by Richard Downie and later John Nagl to explain the (in)ability to learn from experience, Grissom argued that these works had reduced "the bottom up characteristics of organizational learning . . . to information gathering."[21]

Grissom's encouragement to study bottom-up innovations during war fell on fertile soil. Empirical studies on how deployed units adapted to operational challenges in Iraq and Afghanistan have burgeoned. The troops at the sharp end of the conflict had to cope with insurgencies and were therefore often the agents of change.[22] Invariably, Western armed forces were woefully underprepared in terms of doctrine, training, and equipment.[23] Regardless of the institutional response to these deficiencies, servicemembers in the field had to improvise to get by the perils of conflict.

Besides the attention toward adaptations in conflict, other trends in military innovation studies are discernible. The influence of strategic and organizational culture on military change has become more pronounced.[24] Another trend is the increased attention toward how irregular forces adapt in war.[25] This is a welcome development as it enhances our understanding of adversaries. A final, albeit modest trend, is renewed consideration for applying elements of organizational learning literature as a conceptual model.[26]

Unmistakably, the literature on military innovation—or adaptation—has grown and evolved since Grissom's article. This was recognized by Stuart Griffin in 2017, and he lauds the flurry of in-depth research being conducted by scholars on military innovation. According to Griffin, this deluge of academic work on military innovation and adaptation is made possible by the openness of Western militaries in a quest to better understand organizational culture and the dynamics of innovation. The main benefit of this development is that this has yielded an abundance of empirical data. He ascribed this interest to the uncertainty within militaries about the ability to cope with current and future threats.[27] Yet, Griffin also identified challenges that the field of military innovation must overcome. He contends that the pursuit for understanding innovation has led to an infusion of conceptual models without sufficient reflection of whether these are valid to the field. Even more profoundly, Griffin ponders the question of whether military innovation constitutes a separate academic field. He contends that much of the research is essentially concerned with organizational learning rather than "innovation." Furthermore, while armed forces have distinct characteristics, particularly in war, the similarities with other (bureaucratic) organizations are equally prominent. Finally, by positioning military innovation studies as a discrete field, it becomes isolated from theoretical developments in organization studies that could potentially be beneficial to it.[28]

In sum, the literature on military adaptation has evolved significantly during the last decades. Empirical studies on bottom-up adaptation have proliferated because of recent wars. Still, theoretical issues remain. The next section will assess how *Adaptation under Fire* and *Learning the Lessons of Modern War* contribute to this body of literature.

The Merits of Recent Additions to the Field

Barno and Bensahel's *Adaptation under Fire* and Mahnken's *Learning the Lessons of Modern War* are thoroughly researched and accessibly written books. Of course, as mentioned in the introduction, the books have different aims and perspectives. As such, they are complementary to each other and can be read in conjunction. While *Adaptation under Fire* focuses on the American experiences in Iraq and Afghanistan, *Learning the Lessons* offers a more diverse array of cases, including British and Iraqi perspectives and studies on recent conflicts such as in Georgia, Sri Lanka, the Philippines, and Colombia.

Taken together, the books can serve as great introductions to military adaptation and the lessons of recent conflict with both sufficient breadth and depth. At the same time, it is important to note that in the empirical research no new ground is broken between these recent works. For *Learning the Lessons of Modern War,* Thomas Mahnken has found an impressive array of scholars for the individual chapters. Among others, Williamson Murray, Ahmed Hashim, Theo Farrell, Douglas Porch, and T. X. Hammes have contributed to this volume. Many of these chapters are reiterations of earlier works by the authors. These observations for both books are not intended as a critique, as the quality of the work is apparent. Still, for readers who are well versed in recent conflicts and military adaptation, the books hold little new empirical data. For new students on these subjects, these new works form invaluable introductions.

Central to *Adaptation under Fire* is what the U.S. military's exertions to overcome the operational challenges in Iraq and Afghanistan say about its ability to adapt in future conflict. Barno and Bensahel contend that adaptability is a crucial tenet in war. Invariably, militaries have a predilection to make the wrong predictions about the localities, adversaries, and characteristics of future wars. Hence, if the future cannot be predicted, the organizational flexibility to overcome strategic and tactical shocks are paramount.[29] The ability to adapt is even more pronounced through the existence of a thinking adversary that actively seeks to thwart the plans through virtually all available instruments, including lethal force. Moreover, the authors posit that the requirement for adaptability will only become more pertinent for future wars.

Barno and Bensahel elaborate on this proposition by identifying three drivers for what they call a growing "adaptation gap." First, there are the myriad of potential adversaries, including great power competitors, regional actors, and violent nonstate actors. Furthermore, global events can add to the volatility, such as climate change, mass migration, and increasing urbanization. A second driver is the recent addition of two domains of war: outer space and cyberspace. The consequences of war in these domains cannot yet be gauged through a lack of empirical data. Nevertheless, the U.S. military must come to grips with operating in these domains. A final driver is the increasing scale and pace of technological developments. The emergence of artificial intelligence, robotics, and new weapon systems will affect the character of warfare. The combination of these drivers further compounds the problem of predicting war and consequently increases the need for adaptability in conflict.[30]

Against this analysis of future challenges, Barno and Bensahel seek to assess the recent track record of American adaptations in the wars in Iraq and Afghanistan. To examine the case studies, the authors establish a theoretical framework on military adaptation, using the most prominent works in this regard. Interestingly, *Adaptation under Fire* does not explicitly include organizational culture in its analytical framework. This is not to say that Barno and Bensahel discount culture as an influencing factor on organizational adaptability. Rather, they use a framework that consists of doctrine, technology, and leadership as practical manifestations that are shaped by organizational culture.[31] Although this analytical framework is not novel, the application of these distinct manifestations of adaptation processes ensures a broad understanding of this phenomenon.[32] A further strength of the proposed framework is that the authors examine both tactical and institutional adaptations and seek how these two levels interact.[33]

Although their framework chapter is concise yet comprehensive, some points from the literature warrant more critical engagement from the authors. For instance, Barno and Bensahel reiterate the proposition by Michael Howard that militaries are built to fight and win wars, but that they are called to do so rarely. When war breaks out, armed forces can test their assumptions, concepts, and technologies through the crucible of combat. Training exercises and studying military history can offer alternative ways to gain insights, yet these are mere substitutes for the feedback provided by war.[34] Williamson Murray posits that militaries are reluctant to change because the stakes can be existential for militaries and the nations they serve, which ostensibly impacts military adaptation.[35] However, while reading these classic axioms and considering the wars of the early twenty-first century, one can query the applicability of them to recent history. The U.S. military and allied forces have continuously been engaged in conflicts for the last two decades, albeit in varying intensity. As a result, there is continuous feedback of the efficacy of operations and potential basis for organizational adaptations. Second, the conflicts that Western militaries have recently been engaged in did not pose an existential threat, despite all the challenges these organizations faced.

The latter point ties in with the conclusion of the book. Throughout the work, Barno and Bensahel compellingly show that the institutional response to identified deficiencies left much to be desired. Indeed, a main reason for failed institutional adaptations is that the organization prioritized potential future wars over current conflicts.[36] One of the more salient observations that can be derived from *Adaptation under Fire* is that creative tactical adaptations by deployed American units were rather successful. Evidently, for troops, combat deficiencies in organizational performance may well form an existential threat. Conversely, institutional responses were often stymied by bureaucratic inertia and reluctance, ostensibly based on the need to be ready for other threats. This chasm between tactical and institutional adaptability is powerfully driven home in the chapter on technological adaptation. Although the authors repeatedly identify this lack of urgency at the institutional level, they do not explicitly incorporate an analysis of the perceived character of the wars in Iraq and Afghanistan in their theoretical framework.

The other case studies in the book are equally engrossing reads as the authors examine the processes in a clear and convincing manner. By analyzing doctrine, technology, and leadership, a comprehensive, albeit troubling picture emerges about the state of American adaptability. For instance, the analysis of the development of new counterinsurgency doctrine shows that successful institutional adaption hinges on bypassing normal procedures. Moreover, the drafting and implementation of the doctrine "required several stars to almost perfectly align."[37]

For the case studies, Barno and Bensahel mostly use secondary literature to provide an analysis of American efforts to adapt. As described in the previous section, the authors can draw on a wealth of literature. Salient sources that are extensively referenced in this regard are institutional analyses such as *A Different Kind of War* (2010) by Donald P. Wright on the early stages of Operation Enduring Freedom and the two-volume study *The U.S. Army in the Iraq War* by Colonels Joel D. Rayburn and Frank K. Sobchak. Such internal studies form invaluable sources for examining adaptation. Barno and Bensahel deftly use these and other available sources for their analyses. The manifest familiarity with the operations and the U.S. military as an institution pervades the book and pleasantly adds to the readability. An additional strong aspect of *Adaptation under Fire* is the penultimate chapter that serves as the conclusion. It analyzes the underlying causes that impede adaptability in doctrine, technology, and leadership.

A final point of observation on *Adaptation under Fire* is that the authors repeatedly warn against the assumption that future wars will resemble those of the past.[38] This is what William C. Fuller Jr. designates as "the fallacy of linear projection."[39] Fuller also identifies the mirror image of this fallacy, which he calls "the notable exception." This represents the idea that a previous war should be considered an anomaly and consequently holds no relevant lessons for the future.[40] A classic example of this fallacy is the rejection by the U.S. Army of its counterinsurgency experience after the war in Vietnam. Barno and Bensahel describe this episode as it left the United States unprepared for the challenges in Iraq and Afghanistan.[41] However, regarding these latter wars, the authors stress the differences with potential future warfare and that the U.S. military should be wary of the lasting imprint of the recent conflict.[42] This analysis certainly has merit, in particular concerning capable adversaries and fighting under austere conditions. Still, an inquiry on what relevant lessons can be gleaned from recent conflicts is germane, if only to avoid repeating the mistakes from Iraq and Afghanistan.

The relevance of the experiences of recent conflicts is more pronounced in Thomas Mahnken's edited volume, *Learning the Lessons of Modern War*. The chapters by Michael Evans and Williamson Murray contend that a thorough grasp of history can help inform judgment on current affairs. Furthermore, history is the only support we have in preparation for the future.[43] This is not to say that history holds clear-cut lessons, but it can serve as a frame of reference for future wars in which new concepts and technologies can address identified past and future challenges.

A recurring conclusion in the book is the centrality of information in modern conflicts. Despite the abundance of available information in the twenty-first century, armed forces have had difficulties to leverage this information. For instance, Peter Mansoor states that the United States initially lacked both a sufficient understanding of the environment in Iraq and the ability to conduct effective information operations.[44] Furthermore, the Western penchant to assess missions through quantitative metrics generally obscured the understanding of conflicts.[45] Another observation is that during these wars, the deployed armed forces started with outdated conventional approaches that emphasized kinetic engagements. In most cases, these did little to defeat the adversaries or were even counterproductive. Only gradually did the militaries enhance their capabilities for nonkinetic engagements.[46] Perhaps the most important observation that can be derived from these wars is that armed forces with a narrow kinetic focus are bound to be unsuccessful. Instead, the military must be employed in close cooperation with other instruments under clear political guidance.

In this regard, the chapter by Todd Greentree on interagency cooperation in Afghanistan forms a highlight in the book. It describes how the various U.S. government agencies tried and largely failed to produce a common and comprehensive strategy for Afghanistan. Despite efforts to establish coordinating bodies in Washington and Kabul, the beneficial effects were negligible. The multitude of agencies competed for influence and often pursued contradictory objectives. Beyond the lack of cooperation, Greentree concludes that civilian contributions were both quantitatively and qualitatively insufficient.[47] The inability to foster effective civil-military cooperation in expeditionary missions must serve as a stark warning for future conflicts.

Other significant chapters are those by Ahmed Hashim and Douglas Porch, examining the counterinsurgencies in Sri Lanka and Colombia, respectively. The case of Sri Lanka details how the insurgency by Tamil rebels was defeated by government forces. While adaptations helped to tip the balance toward the counterinsurgents, Hashim's observation that the government simply did not have the luxury to withdraw from the conflict is crucial. Arguably faced with an existential threat, the Sri Lankan government had a straightforward strategy with which it could deploy its military.[48] Porch's chapter on Colombia is relevant as it underwrites the primacy of political considerations in war. Although the counterinsurgency campaign of Plan Colombia was militarily effective in defeating the insurgents of the Revolutionary Armed Forces of Colombia (FARC), this was not followed by a viable political settlement. Moreover, military activities (supported by the United States) did little to address the root causes of Colombian instability.[49]

In the short conclusion of the book, Mahnken seeks to draw general themes from the case studies on modern conflicts. Naturally, he reiterates the importance of history to the military profession. The other observations pertain to how military organizations learn. This starts with understanding the environment, the adversary, and the dynamics of the conflict. Assessing the progress of a mission is therefore crucial to identify deficiencies (or opportunities), yet the actual situation is often obscured by flawed metrics. To translate observations on organizational weaknesses into action requires time, attention by leadership, and institutional clout. Finally, it is important to acknowledge both the unique aspects of a conflict as the general nature of war.[50] These observations show that while learning from conflict is crucial, it is also inherently difficult. Additionally, the identified themes point to potential further research. Given the breadth of the case studies and the significance of the identified themes, Mahnken's conclusion is too concise. The book would have benefited from a more extensive ending for tying the chapters together and elaborating on the observations.

The State of the Literature and Potential for New Research

The new works *Adaptation under Fire* and *Learning the Lessons of Modern War* have substantial merits and are welcome additions to the field. On their own, they can serve as great introductions to the study of military adaptation and recent conflicts. When read in conjunction, the value of the books is enhanced, despite considerable overlap in the case studies. Together, *Adaptation under Fire* and *Learning the Lessons* offer diverse perspectives, a breadth of case studies, and different academic approaches. As such, the books are recommended readings, in particular for new students of the field.

As can be derived from the preceding sections, the empirical and theoretical contributions of the books are limited. This observation is not to be construed as harsh criticism of these new works. The authors set out to attain different objectives with their publications. Instead, *Adaptation under Fire* and *Learning the Lessons of Modern War* reflect the current state of the literature. In the last few years, a significant amount of empirical works on recent conflicts have been written, including some institutional evaluations. Of course, analysis of primary sources remains incomplete, in part because of classification. While work remains to be done at this front, the lack of a theoretical foundation continues to hamper the field of military innovation studies.

Adaptation under Fire and *Learning the Lessons of Modern War* do provide inspiration for potential avenues of further research. First, it would be interesting to study the impact of recent combat experiences on the involved armed forces. What adaptations have been institutionalized in the organizations and what have been the underlying processes and analyses for this? What is the informal legacy of the wars of the twenty-first century and how does this affect combat effectiveness? A second subject for potential research is more comparative analysis on how institutional adaptation works, both internationally and across wars in time. Additionally, research should be done on how the institutional perception about a conflict affects adaptation efforts. Do interstate conventional wars have a distinct dynamic of adaptation from expeditionary stabilization operations? Although the apparent return of great power competition commands the attention, Western armed forces continue to be engaged in irregular conflicts.

A final and perhaps most profound subject for research is working toward a synthesis between military innovation studies and the literature on organizational learning. In essence, armed forces are bureaucratic organizations. As Stuart Griffin notes, the study of military organizational change can benefit from the conceptual foundations of organizational learning. How organizations in general interact with their environment and subsequently seek to enhance their performance based on the experience is to a large extent universal. Of course, a conceptual model for studying adaptation and learning in armed forces should account for distinguishing characteristics of military forces, such as the use of kinetic force and the presence of an adaptable adversary. In sum, the study of how armed forces learn and change in relation to conflict remains an interesting academic focus. The value of *Adaptation under Fire* and *Learning the Lessons of Modern War* is that they can attract new students to the field and provide impetus to new research.

Endnotes

[1] Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* 29, no. 5 (2006): 906, https://doi.org/10.1080/01402390600901067.

[2] Stuart Griffin, "Military Innovation Studies: Multidisciplinary or Lacking Discipline?," *Journal of Strategic Studies* 40, nos. 1–2 (2017): 198–203, https://doi.org/10.1080/01402390.2016.1196358.

[3] Williamson Murray, *Military Adaptation in War: With Fear of Change* (New York: Cambridge University Press, 2011), 1–2, https://doi.org/10.1017/CBO9781139005241; Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Delft, Netherlands: Eburon Academic Publishers, 2005), 273–74; and Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Free Press, 2006), 26–28. Cohen and Gooch distinguish between learning and adapting. In their book, the former pertains to lessons from previous wars while the latter designates the process of adaptation in conflict.

[4] Meir Finkel, *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield* (Stanford, CA: Stanford University Press, 2011), 223–26; Lawrence Freedman, *The Future of War: A History* (London: Penguin, 2017), 277–79; and Murray, *Military Adaptation in War*, 5.

[5] Rob Sinterniklaas, *Military Innovation: Cutting the Gordian Knot* (The Hague, Netherlands: Faculty of Military Sciences, Ministry of Defence, 2018), 17–18.

[6] Theo Farrell, "Introduction: Military Adaptation in War," in *Military Adaptation in Afghanistan*, ed. Theo Farrell, Frans Osinga, and James A. Russell, (Stanford, CA: Stanford University Press, 2013), 6–7.

[7] Murray, *Military Adaptation in War*, 1–2.

[8] For a taxonomy of military failures, see Cohen and Gooch, *Military Misfortunes*, 26–28. Essentially, their taxonomy denotes the inability to enact relevant organizational change to overcome operational challenges.

[9] Aimee Fox, *Learning to Fight: Military Innovation and Change in the British Army, 1914–1918* (Cambridge, UK: Cambridge University Press, 2018), 9, https://doi.org/10.1017/9781108120210.

[10] David Barno and Nora Bensahel, *Adaptation under Fire: How Militaries Change in Wartime* (New York: Oxford University Press, 2020), 20–22, https://doi.org/10.1093/oso/9780190672058.001.0001.

[11] Barno and Bensahel, *Adaptation under Fire*, 4.

[12] Thomas Mahnken, ed., *Learning the Lessons of Modern War* (Stanford, CA: Stanford University Press, 2020), 1.

[13] See Barry R. Posen, *The Sources of Military Doctrine: France, Britain and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 224–26.

[14] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), 26–32.

[15] Rosen, *Winning the Next War*, 20.

[16] Richard Duncan Downie. *Learning from Conflict: The U.S. Military in Vietnam, El Salvador, and the Drug War* (Westport, CT: Praeger, 1998), 34–37.

17. Downie, *Learning from Conflict*, 246–47.
18. Grissom, "The Future of Military Innovation Studies," 908–19.
19. Grissom, "The Future of Military Innovation Studies," 919–20.
20. Grissom, "The Future of Military Innovation Studies," 925.
21. Grissom, "The Future of Military Innovation Studies," 926n105. See also John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago, IL: University of Chicago Press, 2002), 3–11.
22. See James A. Russell, *Innovation, Transformation, and War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005–2007* (Stanford, CA: Stanford University Press, 2011); Chad C. Serena, *A Revolution in Military Adaptation: The US Army in Iraq* (Washington DC: Georgetown University Press, 2011); Nina A. Kollars, "War's Horizon: Soldier-Led Adaptation in Iraq and Vietnam," *Journal of Strategic Studies* 38, no. 4 (2015): 529–53, https://doi.org/10.1080/01402390.2014.971947; and David E. Johnson. "You Go to COIN with the Military You Have," in *Insurgencies and Counterinsurgencies: National Styles and Strategic Cultures*, ed. Beatrice Heuser and Eitan Shamir (Cambridge, UK: Cambridge University Press, 2016), 113–48, https://doi.org/10.1017/9781316471364.006.
23. The literature on military adaptation extends to the Coalition forces. See, for instance, Sergio Catignani, " 'Getting COIN' at the Tactical Level in Afghanistan: Reassessing Counter-Insurgency Adaptation in the British Army," *Journal of Strategic Studies* 35, no. 4 (2012): 513–39, https://doi.org/10.1080/01402390.2012.660625; Tom Dyson, "Organizing for Counter-insurgency: Explaining Doctrinal Adaptation in Britain and Germany," *Contemporary Security Policy* 33, no. 1 (2012): 27–58, https://doi.org/10.1080/13523260.2012.659573; Olivier Schmitt, "French Military Adaptation in the Afghan War: Looking Inward or Outward?," *Journal of Strategic Studies* 40, no. 4 (2017): 577–99, https://doi.org/10.1080/01402390.2016.1220369; and Martijn Kitzen, Sebastiaan Rietjens, and Frans Osinga, "Soft Power, the Hard Way: Adaptation by the Netherlands' Task Force Uruzgan," in *Military Adaptation in Afghanistan*, ed. Theo Farrell, Frans Osinga, and James A. Russell (Stanford, CA: Stanford University Press, 2013), 159–91, https://doi.org/10.1515/9780804786768-010.
24. See, for example, Fox, *Learning to Fight*; Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010); Austin Long, *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the US and UK* (Ithaca, NY: Cornell University Press, 2016); and Jeannie L. Johnson, *The Marines, Counterinsurgency, and Strategic Culture: Lessons Learned and Lost in America's Wars* (Washington, DC: Georgetown University Press, 2018).
25. Examples are Noriyuki Katagiri, *Adapting to Win: How Insurgencies Fight and Defeat Foreign States in War* (Philadelphia: University of Pennsylvania Press, 2014); Antonio Giustozzi, *The Taliban at War, 2001–2018* (London: Hurst, 2019); and Chad C. Serena, *It Takes More than a Network: The Iraqi Insurgency and Organizational Adaptation* (Stanford, CA: Stanford University Press, 2014).
26. See Tom Dyson, *Organisational Learning and the Modern Army: A New Model for Lessons-Learned Processes* (Abingdon, UK: Routledge, 2020); Fox, *Learning to Fight*; Frank G. Hoffman "Learning While under Fire: Military Change in Wartime" (PhD diss., King's College London, 2015); and Martijn van der Vorm, *War's Didactics: A Theoretical Exploration on how Militaries Learn from Conflict* (Breda, Netherlands: Faculty of Military Sciences, Netherlands Defence Academy, 2021).
27. Griffin, "Military Innovation Studies," 197–98.
28. Griffin, "Military Innovation Studies," 211–13.
29. Barno and Bensahel, *Adaptation under Fire*, 1–3.
30. Barno and Bensahel, *Adaptation under Fire*, 245–47.
31. Barno and Bensahel, *Adaptation under Fire*, 28.
32. For instance, Williamson Murray alludes to the relations between these aspects. See Murrary, *Military Adaptation in War*, 315–18. Meir Finkel applies this framework to a diverse set of case studies in Finkel, *On Flexibility*, 53–120.

33. Barno and Bensahel, *Adaptation under Fire*, 21–22.
34. Barno and Bensahel, *Adaptation under Fire*, 16.
35. Barno and Bensahel, *Adaptation under Fire*, 16–18.
36. See, for instance, the case study on the mine-resistant, ambush protected vehicles (MRAPs) in Iraq. Barno and Bensahel, *Adaptation under Fire*, 142–55.
37. Barno and Bensahel, *Adaptation under Fire*, 117.
38. Barno and Bensahel, *Adaptation under Fire*, 231–32.
39. William C. Fuller Jr., "What Is a Military Lesson?," in *Strategic Studies: A Reader*, ed. Thomas G. Mahnken and Joseph A. Maiolo (New York: Routledge), 40–43.
40. Fuller, "What Is a Military Lesson?," 43–45.
41. Barno and Bensahel, *Adaptation under Fire*, 103–7.
42. Barno and Bensahel, *Adaptation under Fire*, 260–62.
43. Mahnken, *Learning the Lessons of Modern War*, 19.
44. Mahnken, *Learning the Lessons of Modern War*, 55–57.
45. Mahnken, *Learning the Lessons of Modern War*, 151–52.
46. Mahnken, *Learning the Lessons of Modern War*, 109–15.
47. Mahnken, *Learning the Lessons of Modern War*, 166–68.
48. Mahnken, *Learning the Lessons of Modern War*, 192–95.
49. Mahnken, *Learning the Lessons of Modern War*, 282–84.
50. Mahnken, *Learning the Lessons of Modern War*, 291–93.

National Security Is Still an Ambiguous Concept

José de Arimatéia da Cruz, PhD/MPH

US National Security: New Threats, Old Realities. By Paul Viotti. New York: Cambria Press, 2016. Pp. 326. $35.00 (hardcover).

Providing for National Security: A Comparative Analysis. Edited by Andrew M. Dorman and Joyce P. Kaufman. Stanford, CA: Stanford University Press, 2014. Pp. 340. $90.00 (hardcover); $30.00 (paperback).

Every year, nations around the world release some form of national security strategy document, a so-called white paper. The United States is no exception. The *National Security Strategy of the United States of America* was released in December 2017 by President Donald J. Trump.[1] Despite the many documents released acknowledging a nation's national security, the concept is still as ambiguous today as it was in 1952, when Arnold Wolfers wrote in *Political Science Quarterly* that "national security or national interest. . . . They may not mean the same thing to different people. They may not have any precise meaning at all."[2] Furthermore, as Wolfers so succinctly stated, "the symbol of national security . . . if used without specifications it leaves room for more confusion than sound political counsel or scientific usage can afford."[3] The two books here under review attempt to provide some clarity in the twenty-first century as to what national security looks like, what the new threats are, and why it is

Dr. José de Arimatéia da Cruz is professor of international relations and comparative politics at Georgia Southern University in Savannah, GA. He is also an adjunct research professor at the U.S. Army War College, Strategic Studies Institute in Carlisle, PA, and a research fellow of the Brazil Research Unit at the Council on Hemispheric Affairs in Washington, DC.

still important to pursue a national security in spite of the difficulties of a clear conceptualization of the term.

Paul Viotti, in his book, *US National Security: New Threats, Old Realities,* views national security from a Wolfersian perspective and argues that national security is a highly subjective enterprise. For Viotti, "conceptual understandings about security-related matters . . . are social constructions internalized by decision makers and those who advise them," and therefore the concept is "always subject to multiple interpretations."[4] Viotti views national security as a concept in a state of flux, especially in light of globalization. National security is constantly changing and reinventing itself, depending on ones' perspective. For Viotti, this ever-changing notion of what constitutes national security is partially due to "different understandings, preferences, and exchanges of points of view among decision makers and those advising them [who] become central in what is essentially an intersubjective process."[5]

Viotti's book is divided into two parts. First, Viotti addresses the threats, opportunities, and the use of force. In the new world of the twenty-first century, nation-states have to deal not only with traditional enemies but also a new wave of nontraditional issues including, but not limited to, international organized crime, global climate change, health security, proliferation of weapons of mass destruction, cybercrime, and violent nonstate actors, to name a few. The complexity of the new national security issues is further exacerbated by the fact that a nation's national security priorities must be accomplished "in a still-anarchic, globalized world is daunting."[6] Another important characteristic of national security in the twenty-first century is that there will be many issues that the nation-state will not be able to handle alone. Cooperation will be essential among allies, coalition partners, and other states, in addition to international and nongovernmental organizations.[7]

Arnold Wolfers once stated that "there seems to be no case in history in which a country started a preventive war on the grounds of security."[8] Perhaps that was the case in the old world. In the current world, war still is an instrument of "politics by other means," a la Clausewitz.[9] Today, war will continue to be an instrument of "politics by other means" as well as an instrument of deterrence and coercive diplomacy.[10] While war still is an instrument for achieving a foreign policy goal, the likelihood of conflicts in the future will be dictated by a calculation regarding a balance of terror. That does not mean that military intervention will not take place. War and intervention, as instruments of politics, will continue to be an option in a nation's military arsenal. However, world leaders and their advisers will define what national security is or is not based on, either "construct objectives in relation to what they see as the national interest, [or] some saying, more restrictively, that force should only be used if core values or vital national interests are at stake."[11]

Intervention in the internal affairs of other nations is an integral part of the American experience. How will leaders and their advisers decide when to attack or not attack? Viotti lists eight criteria: objectives in relation to calculations of national interest, likelihood of winning, legal and moral bases for armed intervention, readiness of military forces for deployment, support from allies or coalition partners, expected net effect on the human condition, and degree of public support for armed intervention.[12] While former secretary of state John Kerry announced that the Monroe Doctrine was over, given the United States' hegemony as the lonely superpower in the aftermath of the collapse of the Soviet Union, intervention and war will always be an option on the table for the United States.[13] Nevertheless, the decision to use force will be given much consideration due to its diplomatic, humanitarian, and international implications and unintended consequences, especially as some nations develop nuclear weapons as a deterrence against possible attacks by external forces.

Viotti also discusses the resurgence of insurgency in the international scene as a direct by-product of increasing globalization. While the insurgencies of today are less ideological, especially with the collapse of the Soviet Union and Communism as an ideology, today they are more religiously oriented with the rise of the Taliban, al-Qaeda, and most recently the rise of the Islamic State of Iraq and the Levant (ISIL) and the promise of the caliphate. Viotti defines insurgency based on Bard E. O'Neill's definition, which sees *insurgency* as a

> struggle between a nonruling group and the ruling authorities in which the nonruling group consciously used political force and violence to destroy, reformulate, or sustain the basis of legitimacy of one or more aspects of politics.[14]

Based on this definition, an insurgency's primary goal is to undermine the legitimate authority of the government in power while also legitimizing its own ideology to recruit its own foot soldiers and followers. Viotti argues that insurgencies are highly rational, purposive political enterprise whose existence relies on three key components: its leadership, ideology, and organization.[15] To combat insurgency in the globalized, new world of the twenty-first century, counterinsurgency and intelligence will play a fundamental role. In the context of international relations, *intelligence*, according to Viotti, refers to "the information that governments seek as they monitor and anticipate the actions of both state and nonstate actors."[16]

Given the complexities of new threats and old realities regarding national security in the globalized world of the twenty-first century, no nation-state, regardless of its position within the anarchical international system, will be able to address all of its challenges alone. Cooperation and intelligence sharing will be paramount.

Andrew M. Dorman and Joyce P. Kaufman, in their book *Providing for National Security: A Comparative Analysis*, waste no time describing "what comprises national security remains no less contentious today than when Arnold Wolfers identified the ambiguities within it in the 1950s."[17] The authors' purpose is

> to undertake a comparative analysis of how states are approaching the formulation and implementation of national security. It adopts the premise that although states may no longer monopolize the articulation or provision of national security, they are, in general, still the main protagonists in the formulation and implementation of those policies, and it is through them that the majority of key international organizations, such as the United Nations, NATO, and the EU, work.[18]

Dorman and Kaufman divide their book into five parts. The first part discusses the challenge of national security and the challenges facing the United States in the twenty-first century as the lonely superpower. The second part is entitled "Europe—The Old World." In this section of the book, Dorman and Kaufman examine the national security challenges of France, Germany, and the United Kingdom. Next, the authors examine the challenges facing Australia, Canada, and Japan. Part four discusses the "(Re-)Emerging World," which the authors see as essential challengers to the United States, namely, the "peaceful rise" of China, India, and Russia. The case of Russia is particularly worth reading since this is a fallen superpower attempting to reassert its power in light of the current U.S. retreat or isolationist American first foreign policy approach to world affairs. Part five of Dorman and Kaufman's book, titled the "Potentially (Re-)Emerging World," addresses Nigeria, the Republic of Korea, and Turkey.

Dorman and Kaufman's comparative approach allows national security scholars to "consider how states see their relative position within the international system, how the state security apparatus works, and what factors influence the development and implementation" of their national security policy.[19] The authors' comparative analysis allow scholars to assess the drivers of a nation's foreign policy as well as its history, geography, and political culture. Dorman and Kaufman agree with Viotti that national security in the twenty-first century is more complex. In chapter 2, entitled "The United States' Security Challenges of the 21st Century," they argue that "the challenges facing the United States demonstrate why the country cannot continue to pursue foreign and security policies that simply react to changing world situations."[20]

Dorman and Kaufman do not believe that the United States is the lonely superpower in the twenty-first century. For them, this emerging world will have "multiple power centers that will require some significant rethinking of U.S.

national security policy in order to meet new challenges."[21] A reconceptualization of what constitutes U.S. national security policy is also recommended by Viotti due to new threats such as cybersecurity, international organized crime, human trafficking, and cartels. In fact, Dorman and Kaufman contend that the United States has raised the importance of cybersecurity and the danger posed by cyberattacks by developing, in conjunction with Israel, the Stuxnet virus, which was used to disrupt Iran's nuclear program. Once the virus was identified by the Iranians, they replicated it and released it again, this time against Saudi Arabia's oil companies.[22]

Dorman and Kaufman see the rise of China as perhaps the biggest threat against the United States. They point out that China is highly integrated into the world economy and particularly the U.S. economy, holding enormous amounts of U.S. government debt. According to Kimberly Amadeo,

> The U.S. debt to China is $1.17 trillion as of January 2018. That's 19 percent of the $6.26 trillion in Treasury bills, notes, and bonds held by foreign countries. The rest of the $21 trillion national debt is owned by either the American people or by the U.S. government itself.[23]

While China's economic integration may represent a threat to the United States' position in the world as an economic superpower, it does not mean that China will pursue an adventurous foreign policy and resort to an armed conflict with the United States. China will be more assertive in world affairs as its economic and military power rise, but it will not challenge United States' hegemony as the main security provider in Southeast Asia.

The two books under review see a challenging new world for the United States as it attempts to advance its own national security policy while dealing with new rising threats as well as old threats that now take advantage of a more globalized and networked world. The end of the Soviet Union was much celebrated, especially with the publication of Francis Fukuyama's "The End of History" article, since a common enemy no longer existed.[24] However, after much of the euphoria, the United States and its allies have confronted the reality of some of the new challenges of a new world with new challenges. There are still unknown or *black swan* events—unknown events with catastrophic consequences—yet to materialize in the twenty-first century.[25] As Dorman and Kaufman explained, "there is no agreed or generally unified approach to reviewing defense or constructing a national security strategy or even one that can be associated with [a] particular system of government or style of government."[26]

However, as both Viotti and Dorman and Kaufman stressed in their books, despite the disagreement of precisely what constitutes national security, most white papers released by both the United States and allies emphasize the importance of the 11 September 2001 terrorist attacks (9/11) and the advancement of the Global War on Terrorism. National security is still primarily concerned with the survivability of the state in light of new and old state actors and nonstate actors in world. National security is still written from a realist perspective in its articulation, as pointed out by Dorman and Kaufman, and there appears to have been few inroads from the other international relation's theoretical traditions.[27] Finally, national security is still viewed from a realist tradition perspective of hard power.[28]

Both books provide a fresh perspective on a very ambiguous concept, yet it is one of extreme importance for the survival of the nation-state in light of the tectonic shifts taking place within the post–Cold War system of the twenty-first century.

Endnotes

[1] *National Security Strategy of the United States of America, 2017* (Washington, DC: White House, 2017).

[2] Arnold Wolfers, " 'National Security' as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 4 (December 1952): 481, https://doi.org/10.2307/2145138.

[3] Wolfers, " 'National Security' as an Ambiguous Symbol," 483.

[4] Paul Viotti, *US National Security: New Threats, Old Realities* (New York: Cambria Press, 2016), xi.

[5] Viotti, *US National Security*, xiii.

[6] Viotti, *US National Security*, 23.

[7] Viotti, *US National Security*, 23.

[8] Wolfers, " 'National Security' as an Ambiguous Symbol," 488.

[9] Carl von Clausewitz, *On War*, trans. J. J. Graham (New York: Barnes & Noble Books, 2004), xviii.

[10] Viotti, *US National Security*, 51.

[11] Viotti, *US National Security*, 73.

[12] Viotti, *US National Security*, 74–75.

[13] "Latin America Sees Straight through John Kerry's 'Monroe' Speech," *Guardian*, 21 November 2013.

[14] Viotti, *US National Security*, 122.

[15] Viotti, *US National Security*, 123.

[16] Viotti, *US National Security*, 156.

[17] Andrew M. Dorman and Joyce P. Kaufman, eds., *Providing for National Security: A Comparative Analysis* (Stanford, CA: Stanford University Press, 2014), 6.

[18] Dorman and Kaufman, *Providing for National Security*, 6.

[19] Dorman and Kaufman, *Providing for National Security*, 6.

[20] Dorman and Kaufman, *Providing for National Security*, 13.

[21] Dorman and Kaufman, *Providing for National Security*, 13.

[22] Dorman and Kaufman, *Providing for National Security*, 13.

[23] Kimberly Amadeo, "U.S. Debt to China: How Much Does It Own?," Balance, accessed 13 April 2018.

[24] Francis Fukuyama, "The End of History?," *National Interest*, no. 16 (Summer 1989).

[25] Dorman and Kaufman, *Providing for National Security*, 278.

[26] Dorman and Kaufman, *Providing for National Security*, 279.

[27] Dorman and Kaufman, *Providing for National Security*, 287.

[28] Dorman and Kaufman, *Providing for National Security*, 287.

Beyond Blue Skies: The Rocket Plane Programs that Led to the Space Age. By Chris Petty. Lincoln: University of Nebraska Press, 2020. Pp. 408. $36.95 (hardcover and ebook).

As the nation celebrates recent anniversaries of the Apollo moon flights and the current apogee of man's reach, this book is an excellent tribute to another yet unheralded aerospace effort. This work focuses on the family of experimental rocket planes that streaked across the skies over Muroc, California (later Edwards Air Force Base), providing a treasure trove of scientific, engineering, and technical data. From 1946 to 1975, a myriad of rocket-powered airplanes tested the limits of human endeavor and ingenuity while flying at supersonic speeds on the verge of outer space. From the Bell X-1 to the wingless Bensen X-25A, this book provides a comprehensive history of the experimental airframes and the efforts behind them. This historical treatment is rooted from the perspective of the unappreciated. For this reviewer, the various "X plane" programs were largely overlooked at a time when astronauts, space, and rockets captured the public's imagination. While early American space rockets were routinely blowing up on launch pads, planes like the North American X-15 were regularly entering the realm of space at hypersonic speeds without fanfare.

Author Chris Petty is an aviation enthusiast who runs a blog entitled *The High Frontier*. In his blog, he admits, "I found most interesting . . . aspects of spaceflight that don't always get the spotlight." His self-descriptive observation is reflected in the work as he expertly addresses a history often overlooked, underappreciated, and often relegated to the footnote.

Chronologically organized, the author provides a detailed account of the rocket planes, while also addressing the management and scientific decisions that lead to aircraft development. Petty expertly fills an important void in aviation historiography by discussing how and why these planes were developed, the bureaucratic hurdles overcome, the technical glitches experienced, along with addressing the internal politics of scientific endeavor. While the casual aviation historian revels in the success of Captain Charles E. "Chuck" Yeager and the X-1 or the record-setting X-15's flight of Mach 6.72 by Major William

J. "Pete" Knight, this book delves much deeper into the history of these and other X plane programs. This book provides a refreshing approach to aerospace engineering development that is comprehensive in scope rather than focusing just on salient achievement.

Not only does the work address the success of these endeavors, but he also bravely takes on the failures of various programs. In this effort, Petty explains the fiasco of the Boeing X-20 "Dyna-Soar," the engineering problems with the Bell X-1-3, X-1E, and XLR-99 engines, while including discussion on the various issues with the infamous Bell X-2 costing the lives of two pilots. However, he also addresses the modification and improvement of various airframes and how ingenuity, empiricism, and engineering acumen resulted in success. Petty explains these developments in a manner that the scientific neophyte (as in the case of this reviewer) can fully understand and appreciate. While scientific endeavor is often a trial-and error-process, Petty addresses unfortunate episodes along with crowning success with precision, accuracy, and unvarnished truth.

The work also includes an excellent treatment of the many people involved with these programs. The success (and failures) of the X planes was not just the result of the men in the cockpit, but largely attributed to the skill and acumen of countless engineers, managers, and support personnel who made these planes possible and airworthy. While other authors focus on pilots such as A. Scott Crossfield or Captain Joseph F. Walker, Petty goes beyond the superficial and simple hero-worshiping accounts. Administrators, designers, flight directors, and other lesser-known individuals who made these feats possible are accounted for throughout the book. Petty identifies many of these deserving professionals whose actions were key to the advancement of aerospace technology and the roles these dedicated people played. In this effort, he clearly illustrates the teamwork approach these programs required.

While the book is to be commended for its treatment of management, engineering, and scientific development, this is not necessarily a book for the casual aviation historian. The comprehensive approach delves into details many space enthusiasts might find tedious. Well researched, the bibliography lists an abundance of personal interviews with relevant engineers, managers, and technicians as primary sources. As a result of the author's sourcing of first-person narratives, some accounts tend to be monotonous and appear to be a laundry list of events detracting from the larger work. Regardless, this is only a minor weakness in an otherwise outstanding work.

In all, this is a serious treatment of an often-overlooked part of aviation history. Though usually a footnote subservient to the eventual achievement of the Mercury, Gemini, and Apollo space programs, Petty provides an outstanding account of the rocket-powered X planes. He expertly addresses their success, failures, and more importantly the people who made it possible. Comprehensive in approach and thorough in accounting, this book is a must buy for any serious historian of aviation, space, or technology and worthy of shelf space in their personal library.

John M. Curatola, PhD
Lieutenant Colonel, U.S. Marine Corps (Ret)
Professor, School of Advanced Military Studies, U.S. Army Command and General Staff College at Fort Leavenworth, Kansas

---

Forging the World: Strategic Narratives and International Relations. Edited by Alister Miskimmon, Ben O'Loughlin, and Laura Roselle. Ann Arbor: University of Michigan Press, 2017. Pp. 360. $85.00 (hardcover); $39.95 (paperback and epub).

Introduction: An Essential Follow-up from *Strategic Narratives: Communication Power and the New World Order* (2013)

How can we make sense of the complexity and noise that characterize political communication and international relations today? In taking on such a challenging task and providing an accessible and comprehensive analytical framework grounded in empirical reality, *Forging the World: Strategic Narratives and International Relations* is a tremendous contribution to both the scholarly and policy literatures. With this volume, the editors Alister Miskimmon, Ben O'Loughlin, and Laura Roselle provide an essential follow-up to their seminal 2013 book *Strategic Narratives: Communication Power and the New World Order.* The latter established their theoretical framework and developed the innovative concept of *strategic narrative*, defined as "a means by which political actors attempt to construct a shared meaning of the past, present, and future of international politics to shape the behavior of domestic and international actors" (p. 6). This launched an ambitious and needed policy-relevant research program on strategic narratives, which *Forging the World* brings to the next level.

The Importance of Strategic Narrative Environment: Media Ecologies as "Organic Life-Forms"

In *Forging the World*, the editors and chapter contributors seek to "demonstrate how narratives are used to influence international politics" (p. 2). Indeed, how do we understand how power, communication, and influence align in a globalized world where fake news can influence electoral outcomes, crisis management, and interstate relations? This is one of the key challenges of our time, as evidenced by a recent study that found that online fake news reaches more people than the truth.[1] Strikingly and contrary to conventional wisdom, the responsibility lies not mainly with algorithms and robots but indeed with humans, who have become central actors in the spread of information and indeed of narratives.

Such is the reality of what the editors refer to as our current "media ecology," which they interestingly compare to "organic life-forms" that "exist in a complex set of relationships within a specific balanced environment" (p. 10). That particular analogy is insightful, as the ways in which information spreads among states, societies, and people are inextricably linked to the balance that exists within a given media ecology. Digital disruption has unquestionably challenged that balance, thereby affecting "the distribution and form of authority, legitimacy, and—ultimately—power" (p. 10). The advent of cyber troll armies attempting to drive online discussions and influence trends constitutes one of the latest illustrations of media ecology disruption (p. 11). As the authors point out, the "formation, projection, and reception of strategic narratives" can ultimately only be understood by accounting for the media ecologies in which they circulate and have effects (p. 12).

Main Contributions: How and Why Ideas Become Preponderant on Policy Agendas

In considering the centrality of media ecologies to explain how information and narratives circulate, the editors also interestingly point to the importance of studying "how narratives travel across media ecologies" that are embedded in different cultural and political contexts (p. 12). One of the key contributions of *Forging the World* follows logically from this. The editors build on the observation that it is not sufficient today to show that an idea or narrative starts *trending* or becomes "hegemonic" because the mere presence of an idea or a narrative in the public space is "no guide to whether people like or endorse that idea" (p. 13). Instead, the editors use the concept of strategic narrative as well as their analytical and methodological frameworks in order to demonstrate *how* and *why* an idea becomes preponderant on policy agendas, given media ecology constraints and enablers. In other words, the trending patterns of an idea, a story, or a conspiracy theory (or even of a meme) do depend on a facilitating media ecology for rapid and exponential diffusion. However, this is a necessary yet insufficient condition, especially in the context of international politics. The concept of strategic narrative reminds us that agency and power dynamics are central to the ways ideas spread or *are* spread.

Case Studies: Illustrating Strategic Narratives at Play

Of particular interest to policy audiences is the fact that the editors link their theoretical and methodological frameworks to a large array of well-researched case studies with contributions from key experts from the field. These chapters explore how strategic narratives may help make better sense of the dynamics at play in various organizational, country, and political contexts. This includes great power narratives and their role in identity building (Roselle, chap. 3), the European Union's struggle to narrate with one voice (Miskimmon, chap. 4), and China's strategic articulation of inward and outward-looking narratives (Liao, chap. 5).

Another group of case studies provides interesting insights in how strategic narratives manifest in specific fields. For instance, the domain of international development and the complexity of building "metanarrative[s) of change" in the context of the Millennium Development Goals and the Sustainable Development Goals (p. 157; Sing, chap. 6). This also includes the advent and evolution of public diplomacy and the strategic use of narratives by both terrorist and counterterrorist actors (Brown, chap. 7; Archetti, chap. 9).

Other case studies address the use or misuse of strategic narratives during specific events or crises. For example, looking at the Arab Spring events, Arsenault, Hong, and Price (chap. 8) provide an interesting take on how both internal and external actors use narratives strategically in order to influence the processes and outcomes of a revolution. In chapter 10, O'Loughlin analyzes the Japanese government's difficulties in effectively occupying the narrative space in the wake of Japan's 2011 Tōhoku earthquake/tsunami and the ensuing Fukushima Daiichi nuclear disaster. This shows that for a government, failing to control the narrative not only means the inability to generate a rally-round-the flag type of effect in times of crises but also that other actors may then take advantage of this void to project narratives at the government's expense. That is particularly insightful, especially in light of world governments' struggles to project consistent and convincing crisis-management narratives during the COVID-19 pandemic.

In the book's final chapter, Miskimmon and O'Loughlin build on the many insights developed throughout the volume to make the case that ideas and narratives are critical to understand power transitions and shifts in international order, though they have not so far had a central place within international relations scholarship.

Methodology, Ethics, and How Research on Strategic Narratives Can Inform Policy

Another key contribution of the book lies within its second chapter on "methods and ethics." While the editors' 2013 book established a solid theoretical basis for the study of strategic narratives, it was relatively less comprehensive in providing scholars and students with methodological insights and tools to study strategic narratives systematically. In chapter 2, the editors recall that they approach the study of strategic narratives based on the notion that there "is a spectrum of how persuasion is theorized" in international relations literature (p. 23). That spectrum is based on Brent Steele's four approaches to discourse analysis: rationalist, communicative, reflexive, and poststructuralist. By transposing this framework to strategic narrative research, the authors provide researchers and analysts with a helpful roadmap to study the role and effects of strategic narratives, depending on the research question or phenomenon at hand.

Furthermore, in considering the ethical dimensions behind the policy implications of their theoretical framework, the editors have therefore adopted a rare and welcome approach. Strategic narrative research can inform policy in various ways, and it is crucial that students and researchers alike consider what they are trying to explain and how their research might be used. Indeed, narratives "are not mere ornaments: they do things" (p. 26). Since its publication, *Forging the World* has constituted a major addition to the ambitious research program on strategic narratives set forth by the editors nearly a decade ago.

Overall, *Forging the World: Strategic Narratives and International Relations* is a policy-relevant and civic-minded book, combining academic rigor and accessibility. It provides curious readers with critical and timely insights, helping them make sense of how narratives operate in various political contexts and around complex international issues. Making this type of scholarly endeavors known among nonacademic audiences is essential, as they provide readers with actionable knowledge and key analytical tools. Ultimately, improving education on these issues will constitute the ultimate firewall against the spread and toxicity of fake news and conspiracy theories, which are poisoning our media ecologies, threatening the credibility of our political systems, and endangering the stability of our societies.

Raphaël Zaffran, PhD
Head of learning, program development, and partnerships at the University of Geneva's Centre for Continuing and Distance Education

Note

[1] Soroush Vosoughi, Deb Roy, and Sinan Ara, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 2018): https://doi.org/10.1126/science.aap9559.

It's My Country Too: Women's Military Stories from the American Revolution to Afghanistan. Edited by Jerri Bell and Tracy Crow. Lincoln: Potomac Books, an imprint of University of Nebraska Press, 2019. Pp. 376. $ 32.95 (hardcover); $19.95 (paperback and e-book).

It's My Country Too is basically an extensive and authoritative history of women serving in the U.S. Army and contributing to U.S. conflicts at home and around the world. It follows a chronological arrangement around events unfolding from the American Revolution to the conflict in Afghanistan. The book is conceived as a survey that, due to its clear-cut format and hands-on approach, does not allow the reader to delve deeply into the lives of the women included in order to better investigate their individual personalities. The editors, Jerri Bell and Tracy Crow, as military veterans are well aware that they are dealing with a controversial subject; therefore, the purpose of the book is to connect readers to women and stories both close to their experiences and radically beyond their own, without judging their choices with modern criteria. As they clearly explain in the preface, Bell and Crow present women who chose to serve at various levels in the Army by exposing the salient stages of their military integration, the changes in relevant regulations and execution, and their efforts to pave the way for other women so as to make "women currently serving and those who will follow them to see themselves and their experiences reflected in these pages" (p. xvi).

The anthology presents the proud service of women in the U.S. Army, Marines, Air Force, and Coast Guard as nurses, clerks, engineers, pilots, soldiers, spies but, most of all, it recognizes their contribution in the formation of military units, their tenacity in breaking down barriers, their struggle to work for a lesser pay, their strength to overcome prejudice, and their stamina in performing duties besides their fellow servicemen. The peremptory title "it's my country too" is based on the understanding of war as a highly gendered construct so it is functional to overcome the traditional labeling of women who were first defined as intruders, then as auxiliary officers, and later as invisible veterans. Bell and Crow know it might be misleading to focus only on the conventional polar views of the antifeminist and the feminist, which depict women as "she-roes" or "victims of the patriarchy" since the military context implies a background of contrasting psychological differences between men and women (p. xv). Therefore, they avoid turning these accounts into a contribution history, "which limits its focus to a handful of successful, decorated women who are acknowledged trailblazers" (p. xvi). The editors' real focus is the primary source material and memoir extracts they have curated relying on professional historians in order to separate false claims and legends from documented facts. Bell and Crow have preserved the authenticity of the first-person accounts by assembling a large amount of "memoirs, personal essays, diaries, letters, pension depositions, oral histories, interviews and scholarly histories" (p. xiv). At the beginning of each chapter, they provide a short historical context and add interim periods to inform the reader of the main changes taking place before and between the conflicts. They have also included some photographs of women with brief captions in the central section of the book. The breadth and depth of the autobiographical stories reveal that the book is targeted at a broad audience, which does not only include soldiers, veterans, or insiders but anyone who wants to know women's integration and the evolution of the American military branches.

Bell and Crow present an integration process full of hitches, as each of the armed forces has evolved at its own slow but irreversible rhythm. Women's role in U.S. wars embraced a wide range of activities but the nature of their work was primarily clerical or in support of military medical services. Before 1948, women were members of women's auxiliary corps such as the Women's Army Corps (WAC) and the Women's Army Auxiliary Corps (WAAC), which were formed and dissolved according to personnel shortages. In a conservative and hierarchical system such as the Army, superiority was measured on soldiering and women's participation in wars was jarring and subversive for American society. The editors explain that, accordingly, women were excluded from wartime operations and were not officially in the Army until World War I.

A large part of the book exposes arguments that marshaled against the integration of women into military units. In the first chapter about the American Revolution, the editors express the difficulty in presenting the nature and scope of women's participation, partly because of the loss of the early records and partly because of the male-centered documentation of history since "the stories of women who fought in or supported the Continental Army survived mainly in journal accounts written by men" (p. 3). Women worked in traditional roles as nurses, cooks, laundresses, matrons, or as irregular fighters affiliated with local militia companies. Bell and Crow argue that despite historians' estimates of different female soldiers, writers distorted some stories because they did not endorse the actions of women assuming a man's role as soldiers. They specify that women did not hold military rank, but they were an active part of the armed forces, such as Margaret Corbin, who replaced her husband after he was killed at the Battle of Fort Washington in 1776, or Deborah Sampson Gannett, who enlisted in the Continental Army under the alias "Robert Shurtlieff" (p. 7).

The second chapter informs us that women were initially recruited by the government to serve in the armed forces during the American Civil War. They worked as paid nurses while the majority performed nursing activities as volunteers. Bell and Crow mention that nurses maintained military order within the wards and performed combat support and combat service support functions, but they were not granted military status. Their work was scrupulously scrutinized on and off duty, despite the fact that they voluntarily took on the responsibilities and worked in risky and less visible roles as spies and couriers. Women's wartime contribution did not translate into a formal integration of their capacities and after the war ended in 1865, the Army returned to recruit enlisted men to perform care assistance and nurses went home.

The chapter illustrates the stories of the early female pioneers who have changed the system from within, challenging the basic assumptions about gendered, class, race, and cultural norms to the point of hiding their identities to fight as soldiers. We are immediately hit by the story of Sarah Emma Edmonds who disguised herself as a runaway male slave, shaved her head, and colored her skin to assume the identity of "Frank Thompson" (p. 17). There were also women who engaged in quasimilitary work for regiments next to their relatives, volunteered to wear the uniforms, suffered mental and physical illnesses, and risked their lives to serve their country without the benefits of the men with whom they served. Susie King Taylor, a former illiterate slave, was officially engaged as a laundress and nurse for her husband's regiment but ended up teaching the black troops in the Union Army to read. She states:

> I taught a great many of the comrades in Company E to read and write, when they were off duty . . . I was very happy to know my efforts were successful in camp, and also felt grateful for appreciation of my services. I gave my service willingly for four years and three months without receiving a dollar. (p. 47)

Dr. Mary Edwards Walker crossed multiple boundaries as one of the first doctors in the country, a suffragist who caused a sensation wearing pants. She took up the cause of equal rights advocating for women to serve as soldiers and receive equal treatment both in battle and in pension benefits since "she received a pension half that of her male peers" (p. 41).

The Spanish-American War section is short, but it offers some precious insights into the standards set by the Army. The status of women remained vague, thus penalizing the recognition of their work. In this regard, Esther Vorhees Hasson, a contract nurse, says:

> All applicants will be required to pass a rigid physical and mental examination. . . . Undoubtedly, the future of the Navy Corps will rest largely in the hands of the members, and especially is this true of the first nurses. If they are content with low standards either professionally, morally or socially the status of the corps will be fixed for all time. (p. 64)

In the chapter about World War I, Bell and Crow explain the evolution of women's military corps together with new opportunities for women to take up responsible jobs but also the obstacles to formalize their role. Women were not considered formally engaged in the military and not qualified for veteran status for benefits until Congress decided to professionalize nursing by establishing the Army Nurse Corps in 1901 and the Navy Nurse Corps in 1908 as permanent organizations under the Army Appropriations Act of 1901. Despite personnel shortage contingencies and amid requests for militarization from Army commanders, Congress authorized the Army to appoint women as civilian workers rather than as uniformed members. Their work was still classified as support specialty preventing them to qualify for equal pay, retirement, or benefits. Bell and Crow refer that the Marine recruited women to cover unfilled positions such as clerks (yeomen) and Marine reservists continued to hold a civilian rather than a military rank. Despite the increasing interest in women's roles during World War I, the editors report an episode that reveals the low regard and abuse of authority to which they were subjected. Charlotte Berry, a graduate from the Washington Business High School, proposed to the Navy Secretary Josephus Daniels to enlist women to cover the positions of typists and stenographers. Bell and Crow write:

> The record of the visit lacks detail, and Daniels credited no one but himself for the idea, but Berry later told family members that she had suggested during the call that the Navy enlist women typists and stenographers. (p. 70)

In the imminence of World War II, expansion of the Army to meet the needs of war became, once again, a pressing issue but the staple male rethoric of women as secondary personnel still prevailed over contingencies. The editors stress that nurses were the only corps to be allowed to mobilize; however, the stage for a regular redefiniton of women's service was inevitably set, and it would have repercussions on the public discourse in the following years. The chapter about World War II informs us that 350,000 women served in the armed forces, 150,000 in the Army, 17,000 WACs served overseas, 100,000 served in WAVES (Women Accepted for Volunteer Emergency Service), and thousands of other women served in various military functions within the Coast Guard, the Marine Corps, and the WASP (Women Airforce Service Pilots). Bell and Crow state that in May 1942, the Army was given the authority to establish the Women's Army Auxiliary Corps thanks to the work of Edith Nourse Rogers but only with the status of auxiliary service. Navy WAVES was established in 1942 (the only one to have full military status) followed in the same year by the Semper Paratus—Always Ready (SPAR) within the Coast Guard. In 1943, it was the turn of the WASP. For the first time, women participated in traditional "male" roles and performed technical and scientific tasks as gunnery instructors, flight instructors, and mechanics.

They also contributed as aviators but under the status of civilian employees. After the attack at Pearl Harbor, Congress authorized new women's units for each of the Services and increased the number of active duty positions in the Army and the Navy Nurse Corps.

Despite the fact that the period marked the height of possibilities and range of women's mobilization, activism to grant women military rank overlapped with a smear campaign against them. One of the elements Bell and Crow emphasize is the infamous campaign against the WACs in 1943 aimed at demeaning their reputation and whose effects spread into the other Services. The underlying assumption of masculinity was deeply embedded in the military organizational processes, which in turn led to focusing excessively on women's sexuality. Mary Ellen Graydon, a WAC says:

> One of the most vicious rumors ever started about the WACs surfaced in later 1942. The rumor appeared in the newspapers and on the radio that 250,000 WACs were being sent home because they were pregnant! . . . . To make the situation even worse, highly visible women made a suggestion to the Army that all the WACs be issued condoms! . . . . Our reputation suffered terribly as the result of an awful lie! (p. 107)

She also describes the resulting psychological consequences and the developing of post-traumatic stress disorder (PTSD):

> Later, however, after the war was over, some veterans would learn that our discipline and our war experiences would lead to life-altering physical and mental conditions, later to be called "post-war syndrome." (p. 112)

After the end of World War II, women in the armed forces, except the nurses, were moved to inactive duty. Furthermore, gender stereotypes about women's capacity and ability to engage in "men's work" circulated by the employers and the government. Mary C. Lyne, a SPAR officer, explains how propaganda and magazines helped shape gender stereotypes:

> Attacks upon the morals of SPARs were common . . . tales were invented and improved upon in the telling. . . . Others, blew off steam by drafting letters to magazines and newspapers, secure in their knowledge that the general public, all too suspicious of any innovation, would applaud. (p. 126)

She also points out the competitive pressure between men and women:

> There was many a man whose ego was punctured when he

> found his place could be easily taken by a woman. There was many a man who believed that women should not venture beyond the rose-covered door of the oven. (p. 127)

Women broke the traditional social tenet of the male-female separated dimensions. Josette Dermody Wingo worked as a gunner's mate in the Navy to instruct sailors to fire Oerlikon antiaircraft guns of small caliber antiaircraft artillery. One of the recurring words in the book is credibility, which highlights the importance women attached to professional reputation. Sometimes, they did not have the chance to reach their full potential because they were relegated to civilian roles. Therefore, the decision not to use women in combat positions is the main argument of the following sections.

The chapter about the Cold War reflects the increase in the gender gap and how war and combat further contextualized terms like masculine and feminine. Bell and Crow suggest that the dividing line set between women and men has downplayed the risks and challenges to which women voluntarily exposed themselves. Women's critical skills, such as foreign language mastery, were crucial for foreign missions and helped developing espionage and decryption techniques for coded messages. Bell and Crow point out that women's work helped lay the foundations for the American security agencies; indeed, the WAC "became a recruiting ground for the OSS (U.S. Office of Strategic Services), the forerunner of both the modern Central Intelligence Agency and Special Operations Command (SOCOM)" (p. 130). We discover that Virginia Hall, one of the most famous U.S. spies, risked her life to spy for the Allied forces. Stephanie Czech Radar, one of the first eight women to enter the Women's Army Corps, stood out for her "unusual coolness and clear thinking," which she demonstrated when she promptly handed to a passerby classified material for the U.S. embassy in Warsaw to prevent Soviet security agents from catching it (p. 133).

The Korean War marks one of the most controversial moments in the struggle for women's integration. In this section, women's forgotten service mirrors what has been defined "the forgotten war," thus creating a symbolic intersection (p. 157). During this war only female nurses and medical personnel went to Korea while the remaining part served outside the country, at home, or in Japan. Bell and Crow state that the expansion of women's roles and attempts to increase the number of female soldiers were essentially driven by personnel shortages or shortfalls. But as the Korean War became more unpopular, the number of women within the ranks declined and the enlistment of new women was reduced. After World War II, liberal feminist organizations flourished and feminist policy makers shaped the discourse about enlarging women's rights in addition to commit to securing a professionalized place within the Army. The editors show, through some extracts of the congressional record, the determination of Senator Margaret Chase Smith (R-ME) in the passage of the 1948 Women's Armed Services Integration Act, which gave women permanent status in the military. She states:

> The issue is simple—either the armed service have a permanent need of women officers and enlisted women or they do not. If they do, then women must be given a permanent status. The only possible permanent status is that of Regular status—not Reserve status. Which at most is temporary. (p. 160)

From 1948, the number of women in the Army was fixed to 2 percent, and they were excluded from most of combat and combat support specialties. They could not be employed in operational units to prevent direct contact with combact.

In the chapter on the Vietnam war, the editors note that this conflict marked a moment of stagnation in women's struggle for equal opportunities, both in terms of policies, treatment, and advancement. The notion of women's physical limitation and endurance in combat jobs prevented them from being employed to the front. In the 1960s and 1970s, the feminist organizations led the system to reassess conceptions about gender roles and the division of labor. In 1967, Congress removed the 2 percent limit and restrictions on promotions into higher ranks set by the Women's Armed Services Integration Act.

The chapter affords a glimpse on the objectification of women's bodies and on the blatant double standard applied to women when assessing occupational specialties. Bell and Crow state:

> Recruiters and assignment officers considered physical appearance as a critical attribute. . . . Physical training was intended to keep "women fit and trim" but not to improve their ability to serve in the field. . . . Officers diverted the most attractive women, regardless of their technical expertise, into front-office clerical jobs or protocol. (p. 177)

On the contrary, they highlight that female soldiers can perform as well as men in combat, and they may also overtake men in physical and intellectual abilities even under stressful circumstances as women demostrated in one of the worst attacks of the Vietnam war: the Tet Offensive in 1968.

In this connection, Marine and Intelligence Officer Barbara Dulinsky recalls serving under fire in Saigon during the Tet Offensive and the responsibility of keeping secret documents. Angel Pilato, the first woman Air Force officer in charge of managing an officer's club, explains the discriminatory assumption according to which women were incapable of performing male duties:

> Hightower had put me to the test on the very first day . . . I

> wasn't going to play into any of their preconceived notions of how a woman might run an Officers' Club. (p. 185)

Chapter 9 on gender wars is shorter than the previous ones but summarizes the significant transition that took place within the Army. The 1970s were a turning point for women in the armed forces, both in occupational and symbolic terms since the jobs within the Army became professional positions. Growing female participation led to a considerable change in women' status since they progressed from auxiliary to fully fledged membership and were also authorized to enter the military academies in 1976. Despite resistance and effective incidence on integration, it was a driver of change in the military approach and planning. Bell and Crow also cite the Department of Defense (DOD) all-volunteer force, which initiated the process of wider access to different occupational expertise and doubled the size of its women's programs by 1977.

The 1970s were also years of heated debate and opposition against integration. A major issue raised was the compatibility of effectiveness in military operations and the acceptance of the difference, be it social, physiological, or sexual. Another source of discord was the supposed inability of women to balance the domestic role and the military engagement. Bell and Crow note that there was

> the assumption that military and family duties were inherently incompatible, and the idea that women should prioritize family responsibilities over military duties whenever the two conflicted. (p. 213)

They argue that when women successfully accomplished tasks defined as masculine, a differential yardstick was applied, and they were subject to continuous scrutiny and pressure to prove their physical suitability to suspicious peers and leaders. As a matter of fact, trainings for women consistently improved and new skill areas opened for them since "accusations flew that standards were being lowered" (p. 211). Other problems arose after unit integration collided with the increase of sexual harassment charges and fraternization issues. Navy helicopter pilot Paula Coughlin reports an episode in Tailhook when she faced the so-called gantlet, a kind of assaultive behavior consisting of a group of men who lined the corridor and "grabbed" women on the breasts and buttocks (p. 209). Bell and Crow explain that victims of this male "ceremony," which took place at the Tailook Convention in Las Vega, Nevada, faced great suspicions within the chain of command and were subject to investigations on their psychological stability or to retaliation after reporting it. Even when the harassment was not gender based, new forms of differential male-female assessment emerged, such as the one based on the male physiological structure. The double standard was a discriminating factor making recruits tested for physical strength prior to assigning a specialty. Carol Barkalow, one of the first women to attend U.S. Military Academy at West Point, asserts:

> Women, in particular, became a target group for special hazing, though certainly men were not exempt. The difference was, men had to prove themselves weak before they became subject to this kind of harassment; women had to prove themselves strong before they were spared it. (p. 218)

Through her memoir, we learn that lesbian baiting was one of the practices men used to discredit women by questioning their sexuality:

> We seemed to be continually stuck in a tiresome stereotype—if we were not socializing heavily with male cadets, then it meant we must be lesbians. If we *were* socializing heavily with male cadets, then it meant we must be whores. (p. 219)

She reports other discriminatory behaviors, typical of the conservative male hegemonic attitude:

> Within the cadets' inner circle existed a system of enforcement . . . those who were weak would be wounded and hunted, pushed to the limit to see how much they could stand before they broke down and quit. (p. 223)

The editors point out that these women's accounts are not necessarily representative of every woman's experience but, without them, there would be a partial understanding of their condition or even worse, the risk to have "stories that were once, and are still too often, silenced" (p. 215)

In the chapter about the involvement of the U.S. armed forces and the massive Operation Desert Storm, the editors analyze the controversial issues for and against women's combat exclusion in the light of the modern war context. Operation Iraqi Freedom (OIF) was an outstanding achievement both in terms of the number of women deployed and the nature of their involvement. Mobilization during the 1991 Gulf War involved an unprecedented proportion of women from the active forces, and it was the largest wartime female deployment in U.S. history. Bell and Crow write that more than 41,000 U.S. military women served in key combat-support positions within the theater of the Persian Gulf region. Even though progress was being made toward women's integration, the long-standing opposition to combat roles persisted. In 1988, the Department of Defense Task Force on Women in the Military established the so-called "Risk Rule" to identify and restrict positions and units from which the military Service could exclude women, depending on the mission and location of the job on the battlefield. They cite episodes that cast doubts on the assumption that women were deprived of the physical and mental strength to handle the strain of combat. They provide the examples of Grenada, when women served in Operation Urgent Fury in 1983 in the first gender-integrated units and Panama when they served in Operation Just Cause in 1989 in a variety of combat support and combat service support roles, including intelligence positions.

Objections were also of operational and technical nature, since women were considered as intruders on male bonding and were supposed to have a negative impact on unit cohesion. The editors also provide evidence that, since warfare had acquired a strikingly advanced posture and the real battleground was being played on technological advancement, eventually needs of qualified personnel prevailed over opposition. They refer that "some commanders simply ignored the Risk Rule and assigned women where they were needed" (p. 241). They also emphasize the impact of disruptive elements such as media's reception, distortion, and retelling. Linda Bray's story, the first woman to lead troops into combat, testifies how the capture of the Panamanian Armed Forces dog kennel in 1989 was mediated and misrepresented:

> The politicians weren't paying attention to the actual verbiage that was coming out, so there would be different stories, and there would be conflicting stories of what was going on and what was going on around Panama. (p. 248)

Women felt that media attention was focused excessively on feminine issues rather than on effective contributions and on the impact of arbitrary standards. Darlene Iskra, the first woman to command a ship in the Navy, confesses:

> In early January 1991, my picture and story were on the front page of many international newspapers. . . . Yes, I had worked just as hard or harder for this achievement as my male peers. But what I did not get was the mentoring and advice from my seniors that my male peers received. I was left to fend for myself when I made a mistake or a judgement. (p. 256)

The last section opens in the midst of a renewed climate with significant changes obtained in women's integration. In 1994, the DOD lifted the Risk Rule and replaced it with the direct ground combat exclusion assignment rule, which was aimed at assigning personnel to all positions for which they were qualified in support units. Lauren Kay Halloran, an Air Force public affairs officer, notes how a long-awaited condition had become an unsuspected reality:

> By the time I joined the Air Force in 2006, deployments were the reality of the military service in the post 9/11 era. I wanted to go. (p. 279)

Bell and Crow also highlight the transformation of traditional warfare into asymmetric warfare. In fact, they note that the recent operational deployments in Iraq and Afghanistan under Operation Enduring Freedom and Operation Iraqi Freedom were characterized by less distinct battlefields and nonlinear lines. The forward and rear operating areas were poorly defined so that "support units frequently ended up in close proximity to active engagements or defending themselves from insurgent attacks" (p. 266). The raw reality of this section pulls the reader into the women's personal recollection of the hell they lived. Lory Imsdhal, an Army officer and writer, recalls the harsh reality surrounding her after an explosion in Afghanistan and her dissociation between perception and reality:

> As I ran towards the bridge, I noticed hundreds of shards of skins scattered across the ground like confetti. . . . Sometimes, I tell myself my feelings are simply dormant . . . I told my dad I didn't believe in freak accidents anymore. I'm sure that most argue that this conviction was the stress response of a young lieutenant. I understand my reasons for believing it are based on my feelings, intuition, and personal experience rather than scientific evidence. (p. 300)

Bell and Crow present us the strategies women had to develop in order to cope with individual fears and community expectations. Teresa Fazio, a Marine Corps lieutenant, expresses the stress and shame she suffered to balance the social and professional identity but also the compromises and tactics she used to endure a male environment:

> I was not particularly assertive . . . I accommodated the wishes of other officers around me. The approval I enjoyed for being a "good listener," plus the ease of not having to think too hard, was addictive. I consciously traded what little power I had in order to seem more likeable. (p. 302)

Bell and Crow conclude the book by mentioning further developments in combat exclusion policy, such as the decision by the DOD to rescind the Risk Rule in 1994. Most notably, it established new rules based on gender-neutral standards and equal evaluation parameters built on operational efficiency. They refer that, amid the debate to allow women's full integration and access to all combat jobs, in 2016 Representative Duncan Hunter (R-CA) proposed to amend a defense bill to also require women to register with the Selective Service, although "the measure remains undecided at this time" (p. 314).

The book fulfills the editors' purpose: to inform a heterogeneous public about women's fight for integration and draw the reader's attention to women who "stepped out forward without hesitation regardless of the risk" (p. 317). Bell and Crow respect the principle of authenticity, no matter how hard it is, and frame women in all their complexity and psychological nuances. The assembling work of the editors reveals that they focus more on collectivity rather than individuality, even if this entails lacks or cuts, meaning that little is known about women's single stories and professional evolution. *It's My Country Too* is a highly recommended book, a must-have in any personal collection to keep in mind the value of dedication, as Navy officer Linda Maloney states:

> Become your best at every job you have, even if it's the worst in the command. Strive to be a professional in all aspects of your job. (p. 228)

Sara Ferragamo
Defense and Security Editor at JASON Institute

Iwo Jima and the Bonin Islands in U.S.-Japan Relations: American Strategy, Japanese Territory, and the Islanders In-Between. By Robert D. Eldridge. Quantico, VA: Marine Corps University Press, 2014. Pp. 554. Free (paperback and PDF).

This book is the final part of the trilogy Dr. Robert Eldridge has written, which focuses on the islands the United States had control over after World War II. The islands Eldridge also writes about are Okinawa and Amami Islands, which were in control by the United States for different periods after World War II. The author makes sure to point out that while he is American, he sympathizes with the Japanese family because this book looks at what Americans, Japanese, and other countries did before Japan was able to regain governmental authority over Iwo Jima and the Bonin Islands. By doing this, Dr. Eldridge is showing how where he came from will not change what he sees or perceives in his research. The significance of the United States returning the territory that was seized during the war is huge because it was both a vicious and bloody war.

People remember the battle of Iwo Jima, but many do not know what happened to the islands after World War II. Dr. Robert Eldridge puts all of that into perspective with his book, *Iwo Jima and the Bonin Islands in U.S.-Japan Relations*. This book is a study on the "intra-alliance" dynamics in which one country, the United States, continued to occupy and administer islands that were recognized as Japanese territory but, for several reasons, the United States and its wartime allies felt necessary to continue to administer.

Iwo Jima and the Bonin Islands is broken into four sections that detail how these islands came to be known between America and Japan. The first section looks at the international history and the discovery of the islands. Next is World War II and the fight in the Pacific. The third is the bilateral issues before negotiations on returning the islands to Japan. Finally, the last section discusses the return of the islands. These sections are important because it shows how the dynamic of the countries worked along with each other and against each other. These four sections are integral to the study of the islands in the Pacific because they show the different cultures and how war can change the dynamic. Dr. Eldridge tried to structure the book to capture both the developments and the interplay of the mutual relationship.

Conversely, Japan wanted to prolong the end as long as possible by making sure that the United States could not take Iwo Jima. While Iwo Jima was not a high-value possession to Japan at the beginning of the war, the more reasons the United States wanted to seize the island, the greater necessity it was for Japanese forces to prevent the United States from seizing the island (p. 53). Looking at Iwo Jima and the Bonin Islands are important to study because people can see how the Americans and the Japanese treated the islanders while they lived on the islands and when they were evacuated.

Understanding the relationship between the United States and Japan during and after World War II is important because it shows how each country treated the islands and the people living on them. Both the islanders and the U.S. personnel had mixed feelings when the islands were being returned to the Japanese administration. The U.S. Navy had a different outlook than the American government, meaning that the Navy believed the Bonin Islands should be nonnegotiable and they should not permit any of the repatriations of the former islanders until the islands are reverted. While the Navy did not believe in negotiating with Japan on the Bonin Islands, the United States went ahead and did just that. While Japan was able to get the Bonin Islands back after 60 years of not having control, the return did not resolve all the problems that were present. The way Dr. Eldridge transitions from the U.S. ideologies and Japanese ideologies shows how important both sides and their beliefs are. After World War II, Japan and the United States worked together to find a plan as to what would work best for both countries as well as the islanders. The author was able to show how both the islanders and the U.S. Navy on the island worked among each other while Americans were occupying the Bonin Islands.

Negotiations took time between Japan and the United States, due to both countries wanting different things added on for their countries. One important item was collecting war remains on Iwo Jima. This is important to note because it was the most drawn out and difficult operation that was faced. Collecting the remains of Japanese soldiers started in the early 1950s, and it is still ongoing to this day. Moreover, the author shows how it was not just the Americans' fault that the remains of the fallen were not located. Japanese families had failed in their efforts in trying to locate the remains of fallen Japanese soldiers on Iwo Jima.

In this reviewer's opinion, Dr. Eldridge does a good job of bridging the relationship gap between the United States and Japan. It is interesting that while the author is American, he can remain unbiased while showing what happened on both sides. He conveys both the American and Japanese sides before, during, and after World War II. This gives the reader perspective on both sides and how the islanders lived alongside Americans. This book also unlocks my understanding of U.S.-Japanese relations on Japanese territory after World War II. Overall, this book serves as an essential guide to finishing the trilogy on the three islands in the Pacific Ocean and how their return to Japan changed the relationship between the United States and Japan.

Samantha Boelter, MAH
Independent Scholar

Polymaths of Islam: Power and Networks of Knowledge in Central Asia. By James Pickett. Ithaca, NY: Cornell University Press, 2020. Pp. 320. $54.95 (hardcover); $26.99 (ebook).

James Pickett's *Polymaths of Islam: Power and Networks of Knowledge in Central Asia* is a most welcome addition to the canon of studies about Central Asia, by a clearly talented scholar. This book offers a powerful and vivid history of Central Asia as reflected in the lives of Bukhara's Islamic scholars during the long nineteenth century. But each of those individual concepts, so fundamental to this rich history, require definition. Pickett attends to this right away. "Bukhara the Noble, the Abode of Knowledge" is a city in what is today Uzbekistan. During the period examined here, the polity was ruled by the Manghit Dynasty (1747–1920) and was a center for Islamic learning. Pickett underscores this by noting the degree of high-level study that took place in the city's many madrasas. These 200 institutions of Islamic education were only slightly less in number than those in "Istanbul, capital of the most powerful empire in the Islamic world" (p. 245).

Pickett appropriately sheds light on his title, *Polymaths of Islam*, in the initial pages. His polymaths were ulama, who comprised the patricians of Bukhara—"those who are knowledgeable." In this study they were not simply a stratified caste or reduced to being merely custodians of Islamic institutions and high culture but were simultaneously Sufis, poets, scribes, and scholars of medicine and the law. Pickett's polymaths—Islamic scholars—were each "a jack-of-all-trades, a renaissance man who answered to no one but God" (p. 243). These individual men were remarkable but relied on patronage and were often beholden to members of the Turkic nobility who were warriors of nomadic background. "Turkic dynasts are not the central protagonists of this book, but high culture is impossible without financing, and the ulama cannot be understood separately from their patrons" (p. 245). While Pickett spends time demonstrating that Bukhara was part of the Persianate world, he takes the time to underscore the importance of Turkic languages and culture.

Whereas most authors would distinguish between Sufis and ulama, Pickett demonstrates that they were frequently synonymous. Indeed, he tells us "it is difficult to find an individual scholar of this period who was not engaging in 'sufi' practice of some form or another" (p. 131). But that is the point of this book: to illustrate that Bukhara's scholars were multitalented and multifaceted, "trained in a suite of competencies" (p. 240). Not only did they wear many hats, but they also comprised a clear social group. They were brought together by their common experience of a madrasa education, a "mastery of a canon of texts, and shared regional networks" (p. 243).

Pickett presents his readers with a clear time frame—a *longue duree*—from 1747 to 1920 (the collapse of Nadir Shah's empire and the Bolshevik advance into Turkestan) with several thematic arcs running through this history. Chapters are organized according to these themes rather than chronologically, although he does wrap up logically in 1920. The epilogue takes us just beyond that year, commenting on religion in the Soviet Union through the Cold War.

Polymaths of Islam demands the reader's attention. In addition, this study requires the reader to have some background in Islamic culture (familiarity with the history of Sufism or *din* versus *dunya* for example), Central Asian history (knowledge of Nadir Shah or the "mirrors for princes" genre of literature), and at least a passing acquaintance with Turkic steppe culture. Yet, cohesive introductions and conclusions to each chapter set the reader up for success. One convention that seemed unnecessary, though, was the use of callout boxes. This study's level of sophistication and the background required in a reader obviates the need for such a pedagogical tool.

Pickett undertakes a close examination of sources in Persian, Arabic, Turkic, and Russian languages. He draws on archival research he conducted in Russia (Moscow, Saint Petersburg, and Tatarstan), India, Uzbekistan, and Tajikistan. His sources include memoirs, poetry, biographical dictionaries (*tazkira*), travelogues, notebooks (*jung*), and other manuscripts that defy easy categorization. Additionally, Pickett engages a significant amount of secondary literature, which assists in rounding out his own analysis and puts him in conversation with several fields of scholarship. While *Polymaths of Islam* has clear central considerations and questions, it also comments on a number of subordinate topics. Examples include the definition of Central Asia, the role of the late-nineteenth/early twentieth century reformers known as Jadids, or the etic nature of the concept of Sufism.

With its linguistic and spatial analyses, this book will be of interest not only as scholarship of early modern Islamic thinkers and learning but also of urban Central Asia. Engaging, *Polymaths of Islam* urges the reader to push intellectual boundaries and challenges any simple conceptualizations of Central Asia.

Victoria Clement, PhD
Eurasia Regional Analyst at Marine Corps University's Center for Regional and Security Studies

---

Rhetoric and Demagoguery. By Patricia Roberts-Miller. Carbondale: Southern Illinois University Press, 2019. Pp. 260. $40.00 (paperback and ebook).

In her new book, Patricia Roberts-Miller, professor of rhetoric and writing at the University of Texas at Austin, extends her discussion on the demagoguery practices in American public life from an earlier book, *Demagoguery and Democracy* (2017). In her 2017 book, she emphasized how the American idea of democracy requires Americans to be fair and not to consider that only an enemy's leadership practices demagoguery. Roberts-Miller wrote *Rhetoric and Demagoguery* to point out how knowledge of rhetoric helps equip an American public audience forced to consume U.S. government war information. She is critical of the commercial motivations of American politicians: "In a culture of profit-drive media, demagoguery is, in the short term, a savvy rhetorical strategy." While the rhetoric of demagoguery may make an audience feel "certain, confident, and confirmed," messages that are too complex can cause audiences to turn away from the accompanying ads (p. 4). Americans are too often not given opportunity for real political debate when politicians act like demagogues. Such leaders intentionally mislead by preventing American audiences from any possibility of asking for better information. Demagogues instead offer information containing intentionally hidden designs.

In both her studies on the need to analyze U.S. demagoguery with the approaches offered by rhetoric scholarship, the U.S. 2003 invasion of Iraq is the author's most intense focus because of her concerns that American public intellectuals were intentionally shut out from participating in open deliberation over whether the invasion was necessary. While the author offers many important and convincing historical examples of such demagoguery at work in American public life, she does not adequately identify the original causes for the 2003 Iraq War. Instead, she argues that notions out of Hollywood led to the military attack. Surely a Hollywood script has never motivated those Americans charged with preparing the policies and plans to carry out a real war. But Roberts-Miller thinks such entertainment sources have done so.

In her new book, Roberts-Miller elaborates further on how captive the American audience was as the 2003 invasion took place. She argues that the government chose not to give opportunities for deliberation intentionally: "Americans were invited to eschew deliberating in favor of believing. And we took that invitation" (p. 30). In her view "the Bush administration case for war was, in many ways, not political deliberation, but the plot of an action movie" (p. 43). Rather than be forced into no option but to watch the media reports, "we needed to argue about the plan" (p. 45). This need was forestalled by the intentional cultivation of anti-intellectualism, so that we had to learn facts about Iraq, or about other demagogic controlling historical events, with no supporting evidence (p. 135). Even worse than anti-intellectualism forced on American intellectuals, demagoguery thrives on cultivating anti-deliberative audiences. Furthermore, according to Roberts-Miller, rhetoric joined to demagoguery has the potential for alliteration about what can be the truth: "it says that the truth is easily attained, easily expressed, and easily enforced" (p. 171). One hope for the future is the internet, which has so far proven to refuse to let truth remain constrained and prevents it from being shut down, the way the truth delivered during the newsprint era could be (p. 155).

Roberts-Miller's new book, like her earlier one about demagoguery, succeeds at informing the reader about the power of words and the possibility of demagoguery to destroy a person's life and work through the construction of false claims and no evidence. On the question of the 2003 Iraq invasion, Roberts-Miller insists that there was no rhyme or reason behind the rhetorical rationale readying the reading and viewing audience, without entertaining a shred of doubt that the knowledge of Iraq's willingness to launch attacks on U.S. allies had been confirmed in 1991, when Iraq invaded all the way to Kuwait City and claimed that entire country as one of its oil-producing provinces or from Saddam Hussein's continuing threats to launch rocket attacks on Israel up to 2003. Although no weapons of mass destruction such as nuclear bombs were found in Iraq, the United Nations agency responsible for monitoring such weapons agreed there was the need to go in and search thoroughly to make sure they were not there. Saddam Hussein had imported chemicals such as the components for poison gas and rocket fuel prior to the initiation in 1984 of the United Nations monitoring of all injurious-to-human chemical trade. In sum, my opinion of Roberts-Miller's certain knowledge that, first, there was nothing to any U.S. government or Bush administration assessment of the continuing threat from Saddam Hussein and, second, that the invasion of Iraq should have been less controlled and more openly debated, is that she is applying her beliefs retroactively, which does not really help understand what intelligence was placed on policy making tables, scrutinized and evaluated, that led to the invasion. We need such intelligence to be made public, or else we are a captive audience for academic beliefs that there was no reason for the invasion.

There should have been more public discussion. At the time there was worry that the embedded journalists who agreed to accompany U.S. invading forces, which the government held out as giving the American audience open access to the conduct of the war, were getting hot and tired, and their reports became full of their discomfort and boredom when very little war came their way. To consider that effort to tell more of the story than eventually was told an intentionally constructed and misleading effort is again 20/20 hindsight. If ever a future invasion occurs, it is hopeful that Roberts-Miller's ideas and demands are influential, so that the American people have media forums to fight any war in advance in order to learn whether they can tolerate future news of failures and fatalities and to what extent those numbers will be entertained. However, that Saddam Hussein was a murderous psychopath who conducted surveillance on Iraqi citizens and terrified them with death threats if he did not control them. It is this reviewer's hope that the U.S. effort in Iraq in 2003 is thoroughly studied by U.S. government bureaucrats to learn what went wrong in the military and in foreign policy. Reading Roberts-Miller book leads to deep thoughts, which our leaders and our citizens need to overcome such failures that unfortunately lead to accusations such as hers.

Beyond her hindsight on the 2003 Iraq War, Roberts-Miller's examples were shocking and convincing about horrifying decisions made by demagogues that harmed many—far too many—Americans. Many Americans have remained ignorant of the reasons for the internment of Japanese-Americans during World War II; Roberts-Miller has done thorough research into its cause. She lays a large part of the blame on the opinion-making power of Earl Warren, the future Supreme Court justice, in both California and Washington, DC, in 1942. Warren later regretted what he caused, an apology that does not lead to any forgiveness for what Roberts-Miller terms the demagoguery of the elite. She also details the terrible effects of charlatan theories about race beginning in the nineteenth century into the twentieth century, which were imaginative concoctions unsupported by science. A number of American and European writers who imagined racial demise through miscegenation and immigration ultimately influenced Adolf Hitler. She identifies the rhetorical constructions, based on ignorance, fear, and anxiety that delusional thinking about progeny and purity, create; her scholarship of rhetoric and writing is valuable because such scholarly identification of rhetorical tropes allows a reader to go in-depth into this literature, without feeling sordid for doing so.

With so much to learn from and so many valuable historical explanations, Roberts-Miller's books are well worth reading. Yet, she needs to consider that there may still be information that needs to be released by the U.S. government to evaluate whether general levels of Iraqi military air force, army, and navy intelligence had flown from Iraq into the hands of U.S. or allied military planners. Sad as it may be to accept, the Iraq War did not originate from a tearjerker Hollywood film plot. Assuredly, there are real reasons to ask the national defense to stop a tyrant from killing anymore. What is really necessary at this point, however, is to look at Saddam's secrets and the extent to which U.S. military and other intelligence agencies received such information. Ascertaining if the information was considered generally credible and verifiable enough to exert ground and air forces against the Iraqi regime, which so brutally oppressed differing religious and ethnic identities, including Kurdish and Christian regions of the country that have yet-to-be-realized national aspirations, is what is really necessary for an accurate critique of why the 2003 invasion of Iraq happened the way it did.

Rhetoric and Demagoguery stirs the reader to try to be a public intellectual who will engage with the available information and study the relevant literature. All Americans need thought-provoking scholars like Roberts-Miller to stay informed enough to participate in public life. She has much to offer that is beyond debate anymore, like the U.S. government transgressions against Japanese-Americans and African Americans. She also has much to offer to provoke questions about why the United States went to war in Iraq in March 2003, although she does not have all the answers.

Ann Luppi von Mehren
University of Memphis

The Secret History of RDX: The Super-Explosive that Helped Win World War II. By Colin F. Baxter. Lexington: University Press of Kentucky, 2018. Pp. 214. $45.00 (hardcover).

Scholarship into World War II continues to unpack the complexity of the Allied efforts to harness science, industry, diplomacy, and organizational culture to defeat the Axis powers. In a fascinating book, Colin F. Baxter, professor emeritus of history at East Tennessee State University, opens a "remarkable, almost forgotten chapter" of the conflict in *The Secret History of RDX: The Super-Explosive* *that Helped Win World War II*. Taking a page from the plea of historian Paul Kennedy to examine World War II "history from the middle," Baxter offers a new perspective on the war by exploring the development and mass production of the world's most powerful explosive then in existence, known as Research Department eXplosive or RDX. Through an Allied effort, "managers, scientists, captains and commanders, and the men and women on the production lines" surmounted "formidable technical and human obstacles" to produce RDX and its descendants of Composition B and Torpex in sufficient quantity to impact the war effort.[1]

First discovered in 1899, cyclotrimethylenetrinitramine, later known as Cyclonite, received study in various countries as an explosive in the 1920s, but the compound's sensitivity and high production costs (compared to TNT) proved prohibitive. In the 1930s, British researchers at the Woolwich Arsenal in London mixed 60 percent cyclonite with 40 percent TNT and beeswax to produce Composition B. With less sensitivity to shock and 30–40 percent greater explosive power than TNT, the researchers at Woolrich confidently believed cyclonite, renamed RDX for security reasons, would prove invaluable loaded in Royal Air Force bombs and Royal Navy torpedo warheads. Production lines at Woolwich and later Waltham Abbey, however, could not produce RDX in sufficient quantity. British leaders, convinced of RDX's importance, looked across the Atlantic for assistance.

In the literal search for more bang for the buck, British need for RDX harnessed research efforts in Canada and the United States. Breakthroughs in the synthesis of the explosive joined with the construction of production facilities in Quebec and in East Tennessee. Baxter centers his book's focus on the latter, the massive Holston Ordnance Works (HOW) near Kingsport constructed by Tennessee Eastman, a subsidiary of Eastman Kodak. HOW, which began production of RDX and Composition B in May 1943, would provide 90 percent of the explosives used by American forces and 10 percent of the British. In another testament to America's industrial might, HOW could produce 577 tons of RDX daily by February 1944, climbing to approximately 700 tons of RDX-rich Composition B by 1945.[2] Baxter's chapter on HOW offers another window into the study of the American home front, with the plant offering economic opportunities for women and African Americans, albeit both subject to unequal pay and the racist inequalities of Jim Crow.

With RDX in quantity, Baxter showcases the impact of the super explosive in the air war over Europe, the Battle of the Atlantic, and in the Pacific theater. American rumors about the danger of Composition B's sensitivity proved a source for mistrust and only 25 percent of bombs dropped by the U.S. Army Air Forces in Europe used the filling. "Had a much larger percentage of bombs been filled with Composition B and been used earlier, the effectiveness of the bombing campaign against Germany might have been greater," notes Baxter, albeit a use prevented by the limited supply of RDX and Composition B.[3] In the form of Torpex (42 percent RDX, 40 percent TNT, and 18 percent aluminum powder), the British 250-pound Mark IX aerial depth bombs proved the deadliest weapon against German U-boats.[4] Under the Pacific, American Mark 14 torpedoes carrying 1,100-pound Torpex warheads delivering an explosive force 150 percent greater than TNT alone devastated Japanese shipping.[5] Fast-burning Composition B, precisely placed around a plutonium core, ushered in the atomic age in the sands of New Mexico and the air above Nagasaki, Japan.

Baxter's cogent writing is supported by an impressive body of international research. From his work at East Tennessee State, Baxter blends his familiarity with Tennessee history and previous research in British military history to outstanding effect to detail the transnational journey of RDX. He draws from multiple archives in the United States, United Kingdom, and Canada and enhances these primary records with a rich array of secondary sources from these same nations. A series of phots are found throughout the text, although a map would have been helpful to place RDX's mass production in geographic perspective. His 36 pages of endnotes contain additional tidbits of information, although issue could be taken that this material is not in the main body of the manuscript, considering its brevity. This is at best a minor quibble.

The Secret History of RDX is an accessible book for a wide array of audiences. This work will prove useful to specialists and generalists of World War II history alike. Baxter has produced a valuable monograph of "history from the middle" and enriched understanding of importance of the triumvirate of industry, science, and Allied cooperation to forge the weapons essential for victory.

Frank Blazich, PhD
Curator of modern military history at the Smithsonian Institution's National Museum of American History

Notes

[1] Colin F. Baxter, *The Secret History of RDX: The Super-Explosive that Helped Win World War II* (Lexington: University Press of Kentucky, 2018), 2, 143; and Paul Kennedy, "History from the Middle: The Case of the Second World War," *Journal of Military History* 74, no. 1 (January 2010): 35–51.

[2] Baxter, *Secret History of RDX*, 3, 105.

[3] Baxter, *Secret History of RDX*, 51.

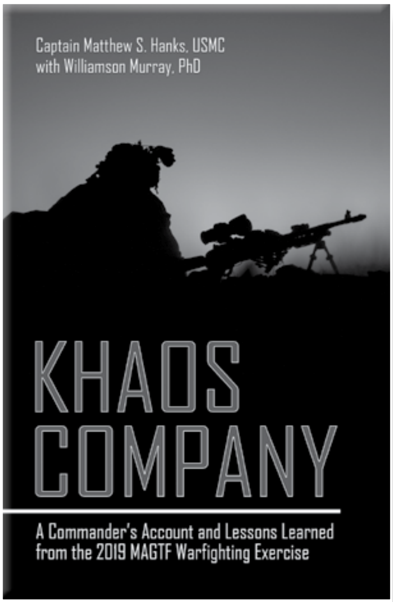
[4] Baxter, *Secret History of RDX*, 133.

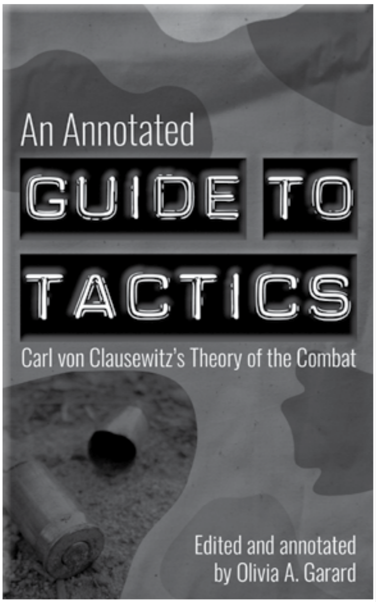
[5] Baxter, *Secret History of RDX*, 84–85.

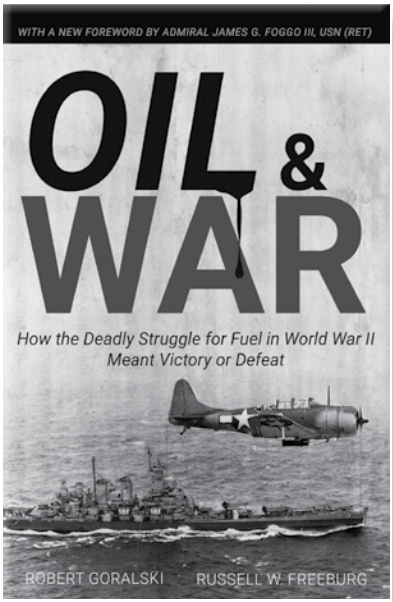
MCUP

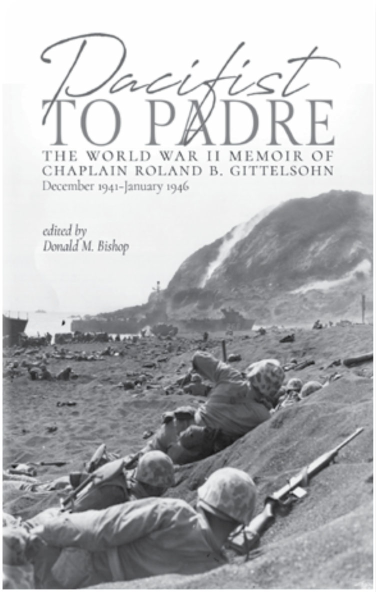
MARINE CORPS UNIVERSITY PRESS

NEW AND


Captain Matthew S. Hanks, USMC
with Williamson Murray, PhD
KHAOS COMPANY
A Commander's Account and Lessons Learned from the 2019 MAGTF Warfighting Exercise

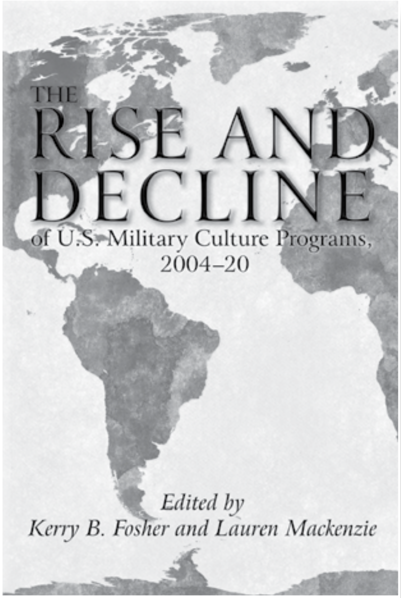

An Annotated
GUIDE TO TACTICS
Carl von Clausewitz's Theory of the Combat
Edited and annotated by Olivia A. Garard

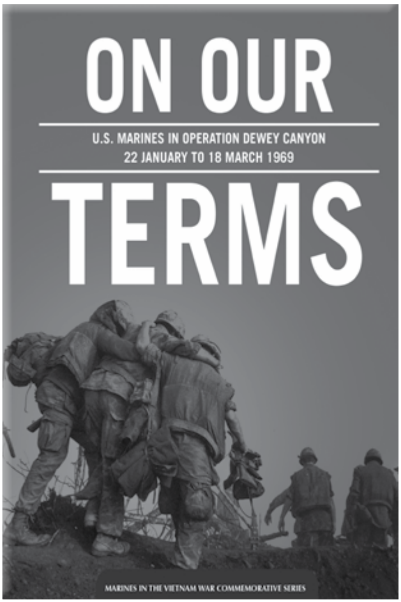

WITH A NEW FOREWORD BY ADMIRAL JAMES G. FOGGO III, USN (RET)
OIL & WAR
How the Deadly Struggle for Fuel in World War II Meant Victory or Defeat
ROBERT GORALSKI
RUSSELL W. FREEBURG

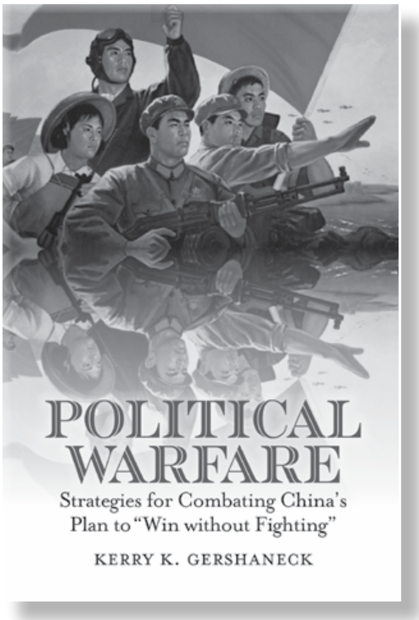

Pacifist TO PADRE
THE WORLD WAR II MEMOIR OF CHAPLAIN ROLAND B. GITTELSOHN
December 1941–January 1946
edited by
Donald M. Bishop

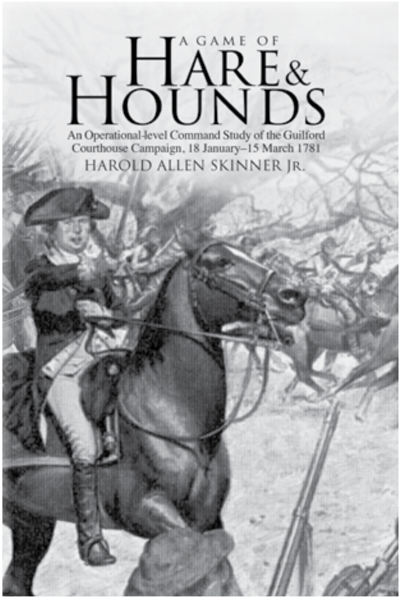
Order your copy by emailing your name, address, and the title(s) to mcu_press@usmcu.edu or visit www.usmcu.edu/mcupress.

FORTHCOMING


THE
RISE AND
DECLINE
of U.S. Military Culture Programs,
2004–20
Edited by
Kerry B. Fosher and Lauren Mackenzie


ON OUR
U.S. MARINES IN OPERATION DEWEY CANYON
22 JANUARY TO 18 MARCH 1969
TERMS
MARINES IN THE VIETNAM WAR COMMEMORATIVE SERIES


POLITICAL
WARFARE
Strategies for Combating China's
Plan to "Win without Fighting"
KERRY K. GERSHANECK


A GAME OF
HARE &
HOUNDS
An Operational-level Command Study of the Guilford
Courthouse Campaign, 18 January–15 March 1781
HAROLD ALLEN SKINNER JR.

MCUP invites authors to submit full-length monographs throughout the year on topics of military science and strategy, military history, national security, and international relations. Visit our acquisitions site for more information.