PERCEPTIONS ARE REALITY

Historical Case Studies of Information Operations in Large-Scale Combat Operations

Edited by Col. Mark D. Vertuli and Lt. Col. Bradley S. Loudon

LARGE-SCALE COMBAT OPERATIONS SERIES

Army University Press

Cover image: The illustration incorporates words associated with Information Operations with a photo of Soldiers from the 350th Tactical Psychological Operations, 10th Mountain Division, conducting a 2008 leaflet drop over villages in Kirkuk Province, Iraq. Photo by Staff Sergeant (USAF) Samuel Bendet.

Original tear graphic: Designed by Layerace/Freepik, freepik.com
Original paper texture: Created by Freepik, freepik.com
Composite cover design: Michael P. Serravo, Army University Press

This book is part of *The US Army Large-Scale Combat Operations Series*, which includes:

Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations

Bringing Order to Chaos: Historical Case Studies of Combined Arms Maneuver in Large-Scale Combat Operations

Lethal and Non-Lethal Fires: Historical Case Studies of Converging Cross-Domain Fires in Large-Scale Combat Operations

The Long Haul: Historical Case Studies of Sustainment in Large-Scale Combat Operations

Deep Maneuver: Historical Case Studies of Maneuver in Large-Scale Combat Operations

Into the Breach: Historical Case Studies of Mobility Operations in Large-Scale Combat Operations

Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations

Perceptions Are Reality

Historical Case Studies of Information Operations in Large-Scale Combat Operations

Edited by
Colonel Mark D. Vertuli and
Lieutenant Colonel Bradley S. Loudon

Army University Press
Fort Leavenworth, Kansas

Library of Congress Cataloging-in-Publication Data

Names: Vertuli, Mark D., 1973- editor. | Loudon, Bradley S., 1974- editor. | Army University Press (U.S.), issuing body.
Title: Perceptions are reality : historical case studies of information operations in large-scale combat operations / edited by Mark D. Vertuli and Bradley S. Loudon.
Description: Fort Leavenworth, Kansas : Army University Press, 2018. | Series: US Army large-scale combat operations series | Includes bibliographical references.
Identifiers: LCCN 2018036198 (print) | LCCN 2018039418 (ebook) | ISBN 9781940804521 (ebook) | ISBN 9781940804521
Subjects: LCSH: Information warfare--History. | Information warfare--Case studies. | Operational art (Military science)
Classification: LCC U163 (ebook) | LCC U163 .P47 2018 (print) | DDC 355.3/43--dc23 | SUDOC D 110.20:7
LC record available at https://lccn.loc.gov/2018036198

2018

Editor
Lynne M. Chandler Garcia

Foreword

Since the Soviet Union's fall in 1989, the specter of large-scale ground combat against a peer adversary was remote. During the years following, the US Army found itself increasingly called upon to lead multinational operations in the lower to middle tiers of the range of military operations and conflict continuum. The events of 11 September 2001 led to more than 15 years of intense focus on counterterrorism, counterinsurgency, and stability operations in Iraq and Afghanistan. An entire generation of Army leaders and Soldiers were culturally imprinted by this experience. We emerged as an Army more capable in limited contingency operations than at any time in our nation's history, but the geopolitical landscape continues to shift and the risk of great power conflict is no longer a remote possibility.

While our Army focused on limited contingency operations in the Middle East and Southwest Asia, other regional and peer adversaries scrutinized US military processes and methods and adapted their own accordingly. As technology has proliferated and become accessible in even the most remote corners of the world, the US military's competitive advantage is being challenged across all of the warfighting domains. In the last decade, we have witnessed an emergent China, a revanchist and aggressive Russia, a menacing North Korea, and a cavalier Iranian regime. Each of these adversaries seeks to change the world order in their favor and contest US strategic interests abroad. The chance for war against a peer or regional near-peer adversary has increased exponentially, and we must rapidly shift our focus to successfully compete in all domains and across the full range of military operations.

Over the last two years, the US Army has rapidly shifted the focus of its doctrine, training, education, and leader development to increase readiness and capabilities to prevail in large-scale ground combat operations against peer and near-peer threats. Our new doctrine, Field Manual (FM) 3-0, *Operations*, dictates that the Army provide the joint force four unique strategic roles: shaping the security environment, preventing conflict, prevailing in large-scale combat operations, and consolidating gains to make temporary success permanent.

To enable this shift of focus, the Army is now attempting to change its culture shaped by over 15 years of persistent limited-contingency operations. Leaders must recognize that the hard-won wisdom of the Iraq and Afghanistan wars is important to retain but does not fully square with the exponential lethality, hyperactive chaos, and accelerated tempo of the multi-domain battlefield when facing a peer or near-peer adversary.

To emphasize the importance of the Army's continued preparation for large-scale combat operations, the US Army Combined Arms Center has published these volumes of The US Army Large-Scale Combat Operations Series book set. The intent is to expand the knowledge and understanding of the contemporary issues the US Army faces by tapping our organizational memory to illuminate the future. The reader should reflect on these case studies to analyze each situation, identify the doctrines at play, evaluate leaders' actions, and determine what differentiated success from failure. Use them as a mechanism for discussion, debate, and intellectual examination of lessons of the past and their application to today's doctrine, organization, and training to best prepare the Army for large-scale combat. Relevant answers and tangible reminders of what makes us the world's greatest land power await in the stories of these volumes.

Prepared for War!

Michael D. Lundy
Lieutenant General, US Army
Commanding General
US Army Combined Arms Center

Contents

Illustrations

Introduction

Colonel Mark D. Vertuli

> *All war is inherently about changing human behavior, with each side trying to alter the behavior of the other by force of arms. Success requires the ability to outthink an opponent and ruthlessly exploit the opportunities that come from positions of relative advantage. The side that best understands an operational environment learns and adapts more rapidly and decides to act more quickly in conditions of uncertainty is most likely to win.*[1]
>
> —Army Doctrine Reference Publication (ADRP) 3-0, *Operations*

Arguably information operations (IO) is one of the most misunderstood and misused terms in Army doctrine—to the point it has largely become a ubiquitous term of reference that lacks the necessary clarity of purpose and application for the majority of the Army. I am sure that if several Army leaders and Soldiers were asked to define information operations in their own words, one would receive several differing—and often conflicting—interpretations. Multiple changes to Army doctrine concerning information operations after it emerged as a concept from Command and Control Warfare (C2W) more than 25 years ago have contributed to this confusion. The definition of IO has changed three times in the last 11 years alone: from a focus on five core capabilities to information engagement (2007), to inform and influence activities (2011), to its current incarnation focusing on information-related capabilities (2016). As the Army shifts its doctrinal focus to large-scale combat operations (LSCO) against peer and near-peer adversaries, the purpose of this volume is to help leaders and Soldiers visualize and understand information operations through the lens of historical case studies.

In both Joint and Army doctrine, information operations is defined as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[2] In more general terms, information operations support the commander's ability to achieve a position of relative advantage through activities in the information environment (the physical, informational, and cognitive dimensions) to influence the adversary's will to fight; disrupt, corrupt, or usurp its capabilities to collect, process, and disseminate information; and ultimately manipulate (deceive) or disrupt an adversary decision-maker's understanding of the operational

environment. Field Manual (FM) 3-0, *Operations* does a very good job describing the broad scope of possible information-related capabilities and effects in the information environment. However, over the course of the last 17 years of counterinsurgency and counterterrorism operations, information operations has become synonymous in many minds with themes and messages, psychological operations (PSYOP)/military information support operations (MISO), or strategic communications/ communications strategy and its larger purpose has become lost. Three lessons—dare I say themes—are interwoven throughout the historical case studies of information operations during large-scale combat operations: (1) the focus is the *information* regardless of the capabilities employed to effect it; (2) successful information operations are operations—integrated, synchronized, resourced and commander-led from inception to execution; and (3) information operations are, at their core, adversary/enemy-focused operations conducted to gain a relative advantage for friendly decision-makers.

"It Is All about the Information"

The title of this volume in *The US Army Large-Scale Combat Operations Series* is *Perceptions Are Reality*. Although this could be a hackneyed phrase, its meaning has great significance to the application of information operations in LSCO. Leaders visualize and understand the operational environment through information. As an element of combat power, information enables decision-making, and its transmission aids decisive operations. Today, modern technology has significantly increased the speed, volume, and access to information. Concurrently, technology has enabled significant means to disrupt, manipulate, distort, and deny information—technology that adversaries have already demonstrated a willingness to use with great effect.

In the book *Dark Territory*, author Fred Kaplan recounts an anecdote from then-Rear Admiral Mike McConnell. While watching the movie *Sneakers* in 1992, the intelligence chief experienced the revelation that "it is all about the information;" that whoever controlled the information could dominate competition and conflict.[3] In LSCO, this remains as true as ever. Leaders direct resources toward intelligence collection in order to develop the situation and gain the sufficient information required to make a timely and informed decision. Just as importantly, measures must be put into place to protect friendly information while simultaneously developing and executing means in all domains to attack the adversary's ability to access, process and disseminate information. In this way information operations enable an accurate understanding of the operational environment while disrupting or manipulating that of the adversary. Through informa-

tion operations, the adversary/enemy decision-maker's reality should be that which best supports achieving a position of relative advantage. The doctrinal definition change away from the rather limiting five core capabilities (Operations Security, Military Deception, PSYOP, Electronic Warfare, and Computer Network Operations) to the current more wide-ranging definition focused on effects is a move in the right direction. That said, more needs to be done to fully garner the true potential of information as an element of combat power in a LSCO context. Common sense dictates that information absent accompanying action does not resonate cognitively in the same way when both are present and complementary. The duality of the relationship between action and information must become a constant theme of operations in the "Information Age" of the 21st Century. However, the perception of information operations as an enabler to maneuver or operations remains.

Information Operations Are Operations

When addressing the idea of conflict in space, the current United States Strategic Command commander, General (USAF) John Hyten, comments that there is no such thing as space war or cyber war, for that matter; just *war*. Similarly, I had a recent conversation with a senior leader who remarked that if information operations planners had their way, everything would be considered information operations. I would like to flip that on its head. During LSCO, maneuver in and through the information environment must be given the same attention as has been historically given to traditional maneuver on the land domain. Maneuver is maneuver and whatever form of maneuver is employed it is done through the operational process.

Recent changes to joint doctrine are beginning to account for the recognition of information's importance in conflict. Just last year, the Secretary of Defense and Chairman of the Joint Chiefs of Staff approved a rapid joint doctrine modification to make information a joint function. More recently, the joint staff issued a directive for operations in the information environment- titled as such to emphasize the activity as operations while avoiding the polarizing term *information operations*. This emphasis comes after observing adversaries wielding information powerfully on and off the battlefield to achieve decisive tactical to strategic outcomes.

In Iraq and Afghanistan, the Taliban and al Qaeda staged countless engagements against United States and its partners, less for the physical effects in the immediate operational environment, but rather to gain an informational advantage around the world. Videotaped improvised explosive device attacks, while devastating, worked well to promote an image

of organizational credibility, bolster adherents' will to fight, radicalize vulnerable populations, and increase financial support. More importantly with respect to LSCO, Russian information confrontation activity preceding, during, and following its illegal annexation of Crimea and invasion of eastern Ukraine demonstrates the power of integrated operations in the information environment, in this case more appropriately term information warfare. Russia successfully sowed disinformation causing the international community to distrust the information it was receiving while also crippling the Ukrainian response through cyberspace operations, electronic warfare, and psychological operations. The confusion and misdirection caused by Russian information warfare had a paralytic effect on Western decision-makers—so much so that Russia was able to achieve its strategic and political objectives before the Western leaders could mount a credible response.

Adversary-Focused

There is one final lesson or theme that runs through the case studies of LSCO: information operations are, at their core, adversary-focused. The 17 years of counterinsurgency and counterterrorism operations gave rise to a population-centric focus for information operations while almost completely subsuming the adversary command and control elements of the doctrine. Only recently—really as a result of adversary successes—has this begun to change. Unified land operations occur in an operational environment dominated by civilians; their presence cannot be ignored or bypassed. However, first, the adversary must be defeated.

Warfare is a human endeavor; it is a contest of wills. The focus of information operations during LSCO must be on defeating the adversary's will. This can be accomplished directly, as during Operation Desert Storm where combined bombing and psychological operations dispirited thousands of Iraqi troops causing their surrender. Or more indirectly, during Operation Iraqi Freedom, US and Allied application of deception, electronic warfare, physical destruction, and cyberspace operations disrupted Iraqi command and control causing an absolute lack of situational understanding and inability to coordinate a defense by Iraqi leadership. As the quote at the beginning of the introduction states: "The side that best understands an operational environment learns and adapts more rapidly and decides to act more quickly in conditions of uncertainty is most likely to win."

The Book

Perceptions Are Reality is composed of 11 chapters. The first 10 chapters explore historical case studies of information operations during LSCO while the final chapter considers the future implications of information operations for LSCO. While many information-related capabilities are explored in the case studies, by no means do they present the definitive accounting. Some of the more technical or sensitive capabilities are not treated in as much depth as I would prefer due to considerations of security and classification. The case studies cover LSCO from World War II through recent conflicts in Georgia and Ukraine. While the United States is prominent in most of the case studies, other nations' operations in the information environment are explored as well, particularly those of the Russian Federation.

In "The Logic of Information Operations in Large Scale Combat Operations," Christopher Lowe explores the evolution of US Army information operations doctrine from its command and control warfare roots to today's commonly held (mis)perception that information operations are a means to influence civilian populations. Colonel Lowe attributes the origin of the United States IO to Cold War Soviet radioelectronic combat doctrine developments. The United States recognized that it needed similar doctrine, organization, training, material, leadership, personnel, and facilities (DOTMLPF) solutions to counter the Soviet's development and an off-set strategy to dominate on the modern battlefield through information. Over the course of several years of peacekeeping, counterinsurgency, and counterterrorism operations, the Army shifted focus from a command and control emphasis to a more population-centric, "hearts and minds" approach. The second chapter continues along a similar narrative.

While Lowe explores IO's past, Justin Gorkowski reflects upon the current state of Army IO in "US Information Operations in Large-Scale Combat Operations: Challenges and Implications for the Future Force." In his chapter, Major Gorkowski details internal structural challenges to Army IO in doctrine, organization, and leadership in juxtaposition to adversarial advancements in the employment information warfare in competition with the United States. While Major Gorkowski's assessment is not positive, it is not without hope for the future. He concludes his chapter with several recommendations to address the imbalance.

The third chapter provides a more in-depth analysis of Russian information warfare. US Military Academy professors Lionel Beehner, Colonel Liam Collins, and Robert Person combine first-hand accounts with secondary research to explore recent historical case studies of Russia's systemic strategic use of information warfare—focusing on the evolution of its military doctrine, from the Russia-Georgia War of 2008 to the ongoing Russia-backed campaign in Ukraine's Donbass Region. This look at Russian strategy of information confrontation offers stark lessons for future large-scale combat operations and the integration of operations in the informational environment to achieve strategic effects.

Taking the approach that one can learn as much from failure as from success, Michael Taylor analyzes one of the lesser-known Allied deception operations from World War II. In "Operation Starkey: The Invasion that Never Was," Taylor explores the reasons for the deception plan's failure to convince German leadership of Allied intentions to invade in 1943 in order to keep German forces in the West and thus relieve pressure on the allied Russian forces in the East. In the following chapter, Branden Riley, Michael Kitchens, and Matthew Yandura use the 1948 Arab-Israeli War to illuminate ways in which information was honed into a weapon by the belligerents and their supporters to achieve desired military, political and social outcomes within the context of large-scale combat operations. In this war, the employment of strategic master narratives to guide operational and tactical maneuver in the information environment proved decisive.

In Chapter 6, Andrew Whiskeyman focuses on the use of Psychological Operations (PSYOP) during the Vietnam War. After a brief exploration of the doctrinal, leadership, intelligence, and organization underpinnings of Military Assistance Command Vietnam (MACV), Whiskeyman details PSYOP employment during the largest ground (Operation Cedar Falls) and airborne (Operation Junction City) operations of the war. While PSYOP achieved some success during these operations, significant challenges impeded widespread support and operational integration. Many of these challenges continue to exist today.

Turning to more recent operations, the next two chapters examine IO during Operations Desert Storm and Iraqi Freedom. First, Robert Hill updates the first chapter of Dorothy Denning's 1992 book, *Information Warfare and Security*. Hill adds a contemporary approach and makes the information relevant to today's operational environment by using editorial comments throughout the text of Denning's exploration of what is considered the first true information war: Desert Storm. In the following chapter, Carmine Cicalese provides the only first-hand account in this volume. As

the Combined Force Land Component Commander (CFLCC) IO planner from April to July 2002, then-Major Cicalese played an instrumental role in the design of information operations to support the CFLCC operational intent. This chapter offers tremendous insight and lessons learned related to planning and executing information operations in LSCO at the highest operational levels.

The final two historical case studies explore elements of cyberspace operations during recent conflicts in Eastern Europe. While Chapter 3 of this volume examines Russian Federation information warfare from a strategic perspective, Wesley White documents Russian operational and tactical integration of cyberspace effects in Georgia, Estonia, and Ukraine. White argues that these conflicts served as test beds—the cyber crucible—for Russian forces to fully integrate cyberspace operations into multi-domain battle. In Chapter 10, Lieutenant Colonel Rick Galeano, Katrin Galeano, Samer Al-Khateeb, Nitin Agarwal, and Lieutenant Colonel James Turner focus on the employment of social botnets in support of military operations. Through detailed analysis of botnet use in Ukraine and the Baltics, they argue social botnet can be used to promote narratives, alter perceptions of viewpoint popularity, and ultimately trigger behavior supportive to military end states.

The volume concludes with a look to the future. In the final chapter, Major General James Mingus and Colonel Christopher Reichart explore the implications of the future information environment across the range of military operations during both competition and conflict. They offer several important recommendations touching elements of Army training, organization, doctrine, and leadership in order to enable commanders the informational capability and capacity to gain and maintain a position of relative advantage in the future operational environment.

The intent of this volume is to employ history to stimulate discussion and analysis of the implications of IO in future LSCO by exploring past actions, recognizing and understanding successes and failures, and offering some lessons learned from each author's perspective. I leave it you, the reader, to determine its success. I want to thank all the authors for volunteering their time and research to support this effort. Brad Loudon provided tremendous advice and editorial support; I could not have completed this without his assistance. Finally, I want to offer my most heartfelt thanks to the leaders at the Army Combined Arms Center and Army University Press for entrusting me with this project.

Notes

1. Department of the Army, Army Doctrine Reference Publication (ADRP) 3-0, *Operations* (Washington, DC: 2017), 1-4.

2. Department of the Army, Field Manual (FM) 3-13, *Information Operations* (Washington, DC: 2016), 1-2.

3. Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016), 31.

Chapter 1
The Logic of Information Operations (IO) in Large-Scale Combat Operations

Colonel Christopher W. Lowe

During the late Cold War, both the United States and the Soviet Union developed sophisticated doctrines in response to their increased reliance on computers, radios, sensors, and other electronic devices for command and control. Known to the Soviets as Radioelectronic Combat (REC), and ultimately, to the Americans, as information operations, these doctrines made the flow and processing of battlefield information an object of war alongside logistics, fires, and maneuver. The cybernetic logic that led to the development of these doctrines—now largely obscured, after decades of irregular war—should once again inform our thinking about large-scale combat operations.

The story of information operations' development begins, not with Sun Tzu or Clausewitz, but with a comparatively recent development in the history of warfare: the "electronic battlefield." In a 1969 address, then Chief of Staff of the Army, General William C. Westmoreland, heralded its coming:

> On the battlefield of the future, enemy forces will be located, tracked, and targeted almost instantaneously, through the use of data links, computer-assisted intelligence evaluation, and automated fire control. With first round kill probabilities approaching certainty, and with surveillance devices that can continually track the enemy, the need for large forces to fix the enemy will be less important.[1]

Apolitical, sterile, errorless, frictionless, devoid of large forces and high casualty rates, Westmoreland's battlefield reads as a vision of everything that Vietnam was not—as the setting for an altogether different, more pleasant, kind of war. In point of fact, Westmoreland's vision was unfolding in Vietnam, and it had already left its mark on battle command during the war. Effective decision making and troop control was, at every echelon, mediated through a host of interconnected and often interdependent, electronic technologies, to include unattended sensors, computers, and radio communications.

Three years earlier, with Westmoreland as senior US commander in Vietnam, Secretary of Defense Robert McNamara directed the develop-

ment of a system to identify and interdict North Vietnamese Army (NVA) movements along the Ho Chi Minh trail.[2] The project, later known as the McNamara line, employed some $670 million in unattended seismic, chemical, and electromagnetic sensors.[3] The sensors transmitted data to overflying aircraft, which in turn relayed this information to an operations center in Nakhon Phanom, Thailand. There, raw sensor data was processed, displayed, turned into targeting data, and furnished to attack aircraft, which could engage and destroy enemy forces in the field.[4]

Ground forces quickly discovered unattended sensors' tactical utility. In 1968, before the McNamara line's completion, the NVA attacked the nearby Marine Corps firebase at Khe Sanh. Westmoreland diverted uninstalled sensors there, a move that, according to one officer, may have reduced US casualties by half.[5] Soon thereafter, units in Vietnam tactically deployed sensors along road networks and around installations.[6]

Military Assistance Command Vietnam (MACV) also relied extensively on computers for intelligence analysis. Under Major General Joseph A. McChristian's direction, the MACV intelligence staff transformed into "a computerized, automated intelligence processing organization" in which over a thousand US and Republic of Vietnam intelligence workers interrogated, exploited, or analyzed enemy prisoners, weapons, documents and other materiel.[7] This "futuristic intelligence system" included the databasing of every captured belligerent.[8]

At the same time, computer systems were showing promise for the purposes of battle command. Under the auspices of the US Army Automatic Data Field Systems Command, formed in 1965, the Tactical Operations System (TOS) was developed and fielded for trial with the US Seventh Army in Germany.[9] Its developers intended that TOS provide the "field Army commander and his staff with relevant and timely information in selected functions of intelligence, operations, and fire support coordination by utilizing an on-line near real-time automatic data processing system."[10]

The use of radio communications also exploded during this time. By 1971, the standard Army brigade maintained 539 radio sets, a massive increase in fielded radios, per brigade, since 1943.[11] In the Korean War, the division headquarters maintained eight channels, in Vietnam, 32—a three-fold increase.[12] Very High Frequency (VHF) radio sets provided reliable communications at lower tactical echelons, enabling units to operate outside of visual range in disruptive terrain.[13] Furthermore, the American Army in Vietnam, for "the first time in history" enjoyed both "voice encryption at the tactical level" and a "fully automated telephone system"

for intra-theater communication.[14] To support the massive communications effort, one of out every five soldiers at the division level was a radio operator.[15]

Maintenance figures further underscore how communications intensive American warfighting had grown. Signal units serviced communications devices at 150 maintenance sites in South Vietnam, where over 500,000 stockpiled communications parts were installed.[16] The criticality of voice communications to modern war was most aptly summed up by General Westmoreland himself, who noted that "on the battlefield no plan of operation is given serious consideration without assured communications. Compare this with the shooting and moving of the mob which has no communication—no control."[17]

During the same period, the Soviet military also increased its dependency on communications and computer networks for command and control. Writing in 1964, Soviet Major General Ivan Kurnosov, chair of the communications department at the Frunze Military Academy, noted that "It is difficult to find a means of combat whose effectiveness to some degree is not dependent upon radio-electronics."[18] Frunze Academy Deputy Chief, Lieutenant General Vasily Gerasimovich Reznichenko assessed that the combination of high mobility platforms and reliable communications would expand, accelerate, and intensify combat operations. Battle, Reznichenko surmised, would be, "characterized by vast spatial range, high dynamism and fluidity, quick changes from one form of combat action to another" and "intensification of critical situations."[19]

Overall, the Soviets appeared to understand the dilemma posed by the electronic battlefield: although information flows increased, commanders enjoyed "less and less time to collect, process, and communicate it."[20] One theoretical option to resolve this problem would be to increase the number of controlling nodes on the battlefield, thereby lessening the span of control. However, as one Soviet officer noted, given the army's size, "this would require an enormous number of staff personnel which, in turn, would greatly complicate the management of such agencies."[21] In other words, from the Soviet perspective, attempts to put more humans in the loop would merely add more complexity.

This complexity, characterized in the Soviet literature as a problem of "troop control" was manageable only with the assistance of computer systems.[22] However, as with any battlefield instrument, communications and computer networks would be vulnerable to enemy attack and the friction of combat. This was significant, as it constituted a vulnerability to the

command and control function itself. In a 1963 *ARMY* article, titled "Command Control and Cybernetics," US Army Lieutenant Colonel Charles J. Davis illustrated precisely this point, describing modern command and control as a nervous system, vulnerable to paralysis and death:

> Picture this "machine-man" on the battlefield. It senses the many events in this environment through the delicate mechanism of sound, light, electromagnetic radiation, and pressure. Myriads of sensory signals, quantitized and at various repetition rates, move down the fine network of "adherent nerve fibers" to reflex centers where they stimulate the first of the reflex arcs. Insufficient processing has taken place to result in intelligent instructions to the effectors of muscles of the system. So the "data" enter the central transmission system—the spinal cord and its amazing trunk of communication lines – on its way to the master processor, the brain. Here, masses of information are sorted, correlated, rejected, and arranged in an orderly array of instructions—orders, if you will—to be sent out over the efferent nerve network to the proper effector elements: hands, legs, arms, feet, eyelids, fingers—the soldiers of the battlefield. Some days the system is sick—pain within, or damage to brain or central nervous system and all response ceases. The thing must be protected—or it dies.[23]

To fully grasp the meaning and implication of Davis' "machine-man" analogy, it's important to better understand "cybernetics," described by its founder as the science of "communication and control." Growing out of his experience in World Word II, Norbert Wiener derived the term cybernetics "from the Greek word *kubernetes*, or 'steersman,' the same Greek word from which we eventually derive our word governor."[24] The wartime challenge that led Wiener to problems of communication and control was the improvement of antiaircraft technology, which aviation technology had lately outpaced.[25]

Increasing aircraft altitude and faster performance meant that air defenders were often unable to visually acquire and engage enemy aircraft passing overhead.[26] Wiener employed the idea of the servomechanism, or feedback loop system, to design a machine that could "predict an airplane's trajectory by making use of information about its previous trajectories."[27] Wiener and colleagues would continue to look to the idea of the servomechanism, or feedback loop system, as a prototype for intelligent machines.[28]

The feedback loop is a circular cause-effect process, by which informational feedback regulates "outputs." A classic example of a negative (or self-regulating) feedback loop is the thermostat. The thermostat "senses" temperature information from the environment, causing it to either raise or lower the output of hot or cool air; a new temperature reading results, causing the thermostat to adjust its output again. This process of feedback and response occurs indefinitely, so long as the thermostat continues to "sense" its environment (in terms of temperature) and can send messages or commands to increase or decrease the flow of heat.

In Wiener's estimation, the "behavior" of the thermostat is little different from the individual human's process of homeostasis:

> [If] our bodily temperature rises or sinks one degree from its normal level of 98.6 [degrees], we take notice of it, and if it rises or sinks 10 degrees, we are all but sure to die. The oxygen and carbon dioxide and salt in our blood, the hormones flowing through our ductless glands, are all regulated by mechanisms, which tend to resist any untoward changes in their levels. These mechanisms constitute what is known as homeostasis, and are negative feedback mechanisms of a type that we may find exemplified in mechanical automata.[29]

With colleagues Arturo Rosenblueth and Julian Bigelow, Wiener described the "behavior" of negative feedback systems, whether man or machine, as purposeful.[30] The common goal of all negative feedback systems, to include mechanical automata as well as living beings, argued the cyberneticists, is to prevent entropy. However, as the thermo-stat and homeostasis examples show, cybernetic systems require an uninterrupted flow of information to balance against entropy. Without continuous information flows, a cybernetic system could neither "sense" the environment appropriately, nor could it command new behaviors.

As Davis expressed it, and as Colonel John Boyd would later (and more famously) describe with his Orient, Observe, Decide, Act (OODA) loop, military forces are information processing systems that continually sense and adapt: "the mission is stated, an estimate of the situation is made, alternative courses of action are considered, a course of action is chosen; orders are issued; the progress of the battle is monitored; and adjustments to the orders are made as time passes."[31] The success of the adaptive cycle—and the outcome of battle, even of the war itself—is determined by the degree to which a force's communications system ensures the flow of

information and thereby, staves off entropy. “Progress is fed back through the area communications system and its complex network of transmission media and switching centers. Using the control information and new battlefield information, another cycle starts—and so on until time is called by defeat of the opposing force or agreement between the national powers.”[32]

The Soviets had long viewed military forces in precisely these cybernetic terms. As Slava Gerovitch contends, Soviet thinkers such as Aleksei Liapunov—one of the Soviet Union’s earliest and most prolific cybernetic proponents—saw “weapon systems, including both machines and the people who operate them as cybernetic systems.”[33] For Liapunov, the military was analogous to an organism, the brain of which was the commander.

As Russia scholar and former Deputy Director of the US Army School of Advance Military Studies, Jacob Kipp, relates, according to Irina Grekova, “one of the leading Soviet specialists in applied mathematics and a long-time professor at the Zhukovsky Academy,” the Soviets were discussing cybernetics as early as 1952, only four years following Wiener’s publication of *Cybernetics or Control and Communications in the Animal World and the Machine*.[34] In 1953, Soviet Admiral A. I. Berg, the newly appointed Deputy Defense Minister, was given responsibility to develop Soviet radio electronics and cybernetics. By 1958, the Soviets had translated Wiener’s Cybernetics into Russian, and a year later, “the Frunze Academy organized a faculty of military cybernetics.”[35]

In the 1960s, after witnessing the successful employment of Electronic Countermeasures (ECM) against Soviet equipment in the Vietnam and 1973 Arab-Israeli wars, the Soviets started integrating various approaches to attack their battlefield opponent’s communications network—that is, to wage a decidedly offensive counter command and control doctrine.[36] The Soviets termed this approach *radioelektonnaya bor’ba*, or in English, radioelectronic combat (REC).[37] After a period of internal debate concerning REC’s “proper nature,” Soviet Major General A.I. Paliy, whom David Chizum refers to as “the Grand old man of Soviet electronic warfare,” published *Radioelectronic Combat*, thereby galvanizing Soviet doctrinal consensus on the topic.[38]

According to Commander (USN) Floyd D. Kennedy, a 1978 US Army study described REC as combining “signal intelligence, direction finding, intensive jamming, deception, and suppressive fires to attack enemy organizations and systems throughout their means of control.”[39] This combination of elements would “limit, delay, or nullify the enemy’s use of his command and control systems” while simultaneously protecting Soviet

systems.[40] REC's most salient feature was its emphasis on integration, entailing the simultaneous combination of multiple protective and disruptive means into a "greater than the sum of its parts" whole, in support of the ground scheme of maneuver.[41] In time, American doctrines would appropriate REC's integrating precept, and it remains today a definitional feature of information operations.

As if the Soviet's sophisticated REC doctrine wasn't threatening enough, the US was woefully outnumbered in raw combat power. Soviet expenditures in military equipment had outpaced US investment by $240 billion in the previous decade, and the principle challenge, evident since the 1973 Arab-Israeli War, was how to fight outnumbered and win. Undersecretary of Defense for Research and Engineering, William Perry's approach was to "counteract a numerical disadvantage in military equipment" through a technological "offset."[42] The "offset" technologies pursued by the Department of Defense under Perry's strategy included "surveillance systems," data communication systems, "positioning systems," and missile "guidance systems"—all dependent, in some fashion, on the electromagnetic spectrum.[43]

The Department of Defense and US Air Force conducted several studies between 1975 and 1978 in light of US plans to invest more heavily in electronic communication technologies that REC doctrine aimed to exploit.[44] These efforts ultimately forged an American version of REC, dubbed Command, Control, and Communications Countermeasures (C3CM), which similarly entailed the integration of Electronic Warfare (EW), Operations Security (OPSEC), Military Deception (MILDEC), and Physical Destruction.

One of the immediate challenges associated with C3CM implementation was the alignment of service doctrine to ensure, in the potential of war, a unified and self-reinforcing C3CM effort across the battle space. To meet this challenge, the Army's Training and Doctrine Command (TRADOC) and the Air Force's Tactical Air Command (TAC) published TRADOC Pamphlet 525-7, *Joint Operational Concept for Command, Control, and Communications Countermeasures (C3CM)* in December 1981. The Joint Operational Concept for C3CM would remain in service for a period of almost ten years, until it was superseded by the Army's Field Manual 90-24, *Multi-Service Procedures for Command, Control, and Communications Countermeasures*, in May of 1991.

The C3CM concept would debut in large-scale combat operations, not on the steppes of Europe, but in the Kuwaiti desert. In August 1990,

Saddam Hussein's Iraqi Army invaded and occupied its neighboring kingdom. The ensuing Gulf War, in which an American-led coalition expelled the Iraqi army from Kuwait and liberated its population, demonstrated the fruit of the US military's technological, doctrinal, and training renaissance of the previous decade. Some also hailed Desert Storm as a proof of concept for a new kind of war, in which information and knowledge played the definitive, if not decisive role. As retired Air Force Colonel and information warfare scholar, Alan Campen wrote, shortly following the war, "knowledge came to rival weapons and tactics in importance, giving credence to the notion that an enemy might be brought to its knees principally through destruction and disruption of the means for command and control."[45] Indeed, the US military did a great deal to destroy Iraqi command and control during the Gulf War, "utilizing a deadly combination of hard and soft kill."[46]

The destruction or disruption of radar sites, air defense systems, command and control centers, electric power nodes, and communications relays effectively severed vital Iraqi information flows, leading many to employ the metaphors of decapitation, blindness, paralysis, and shock in describing the effects of US targeting against the Iraqi Army. For instance, during the war General Colin Powell characterized the "battle plan" as "first to destroy the Iraqis' air defense system and their command, control, and communications to render the enemy deaf, dumb, and blind." Powell noted in a press conference that, "Our strategy is . . . very simple . . . First we are going to cut it off, and then we are going to kill it."[47] In 1993, an Air Force First Lieutenant similarly reflected, "The vulnerability of C2 systems to destruction by air power was demonstrated by the highly centralized Iraqi system. The mixture of Soviet and Western equipment and doctrine was blinded, then paralyzed, then largely destroyed by coalition air attack."[48]

However, it was not only US dominance of the electromagnetic spectrum, whether through physical destruction or electronic warfare, that contributed to Iraqi paralysis. Nearly some 87,000 Iraqi soldiers surrendered as US Psychological Operations (PSYOP) forces targeted Iraqi units with leaflets, loudspeaker scripts, and radio broadcasts.[49] Widespread Iraqi surrender and desertion undoubtedly disabled Iraqi command and control (C2), as it robbed Iraqi high command of its "eyes and ears," contributed to poor morale, and lowered tactical responsiveness. PSYOP appeals provided Iraqi soldiers with the instructions on how to surrender, even if American bombing provided the motivation.

The Gulf War seemed to validate the logic of viewing military forces as cybernetic systems, dependent on information flows for command and control. As the futurist pair, Alvin and Heidi Toffler expressed in their influential book, *War and Anti-War; Survival at the Dawn of the 20th Century*, "The Iraqi forces, especially after most of their radar and surveillance were excised, were a conventional 'military machine' . . . By contrast, the allied force was not a machine, but a system with far greater internal feedback, communication, and self-regulatory adjustment capability. It was, in fact, in part at least . . . a 'thinking system.'"[50]

That the US led alliance achieved this relative advantage was, as Alan Campen, noted, "ironic," as "the Soviet Union—Iraq's prime mentor—was the first to advance the belief that the balance in war might be tipped by attacking the opponent's control structure."[51] A further irony was that the Soviet Union's political control structure was itself dissolving, virtually concurrent with the American-led takedown of the Iraqi command structure. These two events, the near total military success of American forces during the Gulf War and the disintegration of the Warsaw Pact (and with it, the Cold War) would lead to significant reevaluation of threats, opportunities, and doctrine.

Prior to the Gulf War, the Office of Net Assessment (ONA) launched an assessment into the claim, long maintained by the Soviet Union, that a military-technical revolution was causing "a major shift in the character of military competitions."[52] The assessment, titled *Military Technical Revolution: A Preliminary Assessment*, interpreted the "overwhelming US victory in the Gulf War" as evidence that the revolution had, in fact, arrived.[53] However, the assessment also emphasized that the United States was at the "beginning of the revolution."[54] While the United States possessed important technologies, such as precision-guided weapons and information and simulations systems, it was only able to capitalize on "a fraction of their combat potential."[55] This was because "the United States did not come close to its potential to move the most useful information rapidly to those who needed it most."[56]

Introducing language that would later find its way to doctrine, the report asserted, "information dominance could well be the *sine qua non* for effective military operations in future conflicts," and "information superiority could be *the decisive operation* in future conflicts."[57] Furthermore, the report speculated that, since belligerents also understand the decisive nature of information dominance—especially after witnessing the Gulf War—a zero-sum-game phenomenon would likely ensue. To allow en-

emy exploitation of information networks during peacetime would risk enemy information dominance, "which would quickly lead to the progressive inability of friendly forces to execute the highly integrated, information-intensive military operations that will be crucial to success in war."[58] In essence, if the United States failed to maintain continuous information dominance, it would lose the deterrent and coercive power of its military force.

The report asserted that during war the United States would likely achieve information dominance through a "full-dimensional operation."[59] "Strategic strikes (to include so called 'electronic strikes' and special operations forces strikes) against an adversary's terrestrial information networks would ideally be carried out simultaneously with space control operations."[60] As with Soviet REC and C3CM, dominance comes from the destruction of command and control systems.

On the heels of the Gulf War and the ONA's Military Technical Revolution report, the Tofflers advanced the influential thesis, based on their earlier work *Third Wave*, and fully elaborated in *War and Anti-War*, that "the way we make wealth is the way we make war, and the way we make anti-war must reflect the way we make war."[61] According to the Tofflers, history has been characterized by "waves" in which wealth generation and war-making accorded to specific forms.

The first of these waves, beginning in antiquity and largely terminating with the Industrial Revolution, was agrarian. Agrarian war was seasonal, intermittent, unprofessional, and technologically unsophisticated. The Second Wave, brought on by economic industrialization, epitomized mass-production, high lethality, and mechanization. The Third Wave, only emergent at the time of *War and Anti-War*, came with the increasing use of computer technology within the society and the economy. "Knowledge," the Tofflers claimed, "is now the central resource of destructivity, just as it is the central resource of productivity."[62]

This thesis served as a lens through which the Army would view the Military Technical Revolution proposed by the ONA's report. The Tofflers already enjoyed considerable influence within the Army. In 1982, the Tofflers established contacts with a group of influential Army officers, to include the Chief of TRADOC, Commanding General Donn Starry.[63] At the time, Starry was instituting massive doctrinal and educational reforms, to include the development of AirLand Battle and the establishment of the School for Advanced Military Studies (SAMS), both of which later helped to account for the Army's success in the Gulf War. The Tofflers now saw

the Gulf War as the opening campaign of the Third Wave: "Something occurred in the night skies and desert sands of the Middle East in 1991 that the world had not seen for three hundred years—the arrival of a new form of warfare that closely mirrors a new form of wealth creation."[64]

To better understand the ramifications of the Third Wave, the Army turned to the Tofflers directly, inviting Alvin Toffler to deliver a keynote address at the US Army War College's conference, "The Revolution in Military Affairs: Defining an Army for the 21st Century."[65] Furthermore, no less than the Chief of Staff of the Army, General Gordon R. Sullivan, drew on Toffler's insights in developing internal documents, such as *War in the Information Age*.[66]

War in the Information Age championed Toffler's idea that knowledge—translated by the Army as "information"—was becoming the central resource of war. In so doing, its authors reiterated the underlying logic of General Westmoreland's "Electronic Battlefield" and William Perry's Offset Strategy—namely, that more perfect information collection and sharing, enabled by the integration of electronic technologies, would provide a marked advantage over larger Armies.

In the early 1990s, with talk of the Military Technical Revolution, Revolution in Military Affairs, Information Revolution, and Third Wave warfare, the Department of Defense went about updating its now venerable and battle tested C3CM doctrine. By the middle of the decade, the Joint Staff released Joint Publication (JP) 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, which held promise "to shape the adversary commander's estimate of the situation in the theater of operations" and enable the Joint Force Commander (JFC) "to process information through the C2 decision cycle faster than an adversary commander," thereby contributing to Joint Force Information Superiority.[67] In part, as acknowledgement of the contribution that surrender appeals made to the blinding of adversary decision makers in the Gulf War, C2W added PSYOP to the elements formerly associated with C3CM, including EW, OPSEC, MILDEC and Physical Destruction.

However, a new term—information operations—would soon eclipse Joint C2W doctrine. In August 1995, less than a year before C2W's publication, the Army released TRADOC Pamphlet 525-69, *Concept for Information Operations*.[68] In keeping with the Third Wave and RMA discourse, the information operations concept announced revolutionary change. In the pamphlet's forward, General William Hartzog, then TRADOC Com-

mander proclaimed, "The information age paradigm will . . . change the way wars are fought."[69]

Revolutionary proclamations aside, the information operations concept both confirmed and programmatically endorsed the logic underlying Soviet REC, C3CM, and C2W. In language that sounds remarkably similar to Westmoreland's vision of an electronic battlefield, the information operations concept described the upside of digitization and electronic communications: "Digitization will also assist in combat identification and enhance situational awareness through precise friendly and threat signature definition and updating of weapon system recognition software programs. The direct connection between the global grid of communications and the digitized battlefield will allow precision strike operations against high-value targets."[70] However, the functioning of that same "future C2 system" the concept recognized, "is predicated upon our exercising electromagnetic spectrum supremacy or superiority."[71]

In August 1996, a year following the introduction of TRADOC's concept, and five months following JP 3-13.1, the Army published Field Manual (FM) 100-6, *Information Operations*. In keeping with the concept, the new doctrine included Public Affairs (PA) and Civil Affairs (CA) as complementary information operations elements. As with the earlier inclusion of PSYOP within C2W, the addition of PA to information operations seems rooted in the broadly accepted lessons of the Gulf War, particularly with regard to the flow of information not only across but *beyond* the battlefield. The war demonstrated the ubiquity and power of media, which reached global audiences, principally via English language satellite news. This, the doctrine recognized, "can dramatically affect strategic direction and the range of military operations."[72]

Similarly, CA was deemed important to information operations because "of its ability to interface with key organizations and individuals in the GIE [Global Information Environment]; for example, CA's traditional relationship with NGOs and PVOs such as the International Committee of the Red Cross."[73] Furthermore, CA's access to international actors and civilian populations meant that it could serve to both preserve and shape information flows in both the international and local, public communications environments.

During the Bosnia and Kosovo peacekeeping operations, and in the counterinsurgencies of Iraq and Afghanistan, Army forces would look to this expanded information operations doctrine to provide an advantage. However, in these operations, enemy forces, fighting in what Rupert Smith

has termed a "war amongst the people," would largely adopt deliberate strategies that tested the very applicability of information operations' foundational, cybernetic logic. Insurgents, terrorists, and criminal elements, operating in small, decentralized networks, below the so-called "threshold of discrimination," and with low-cunning rather than high technology, rendered the disruption of adversary battle-command somewhat irrelevant, if not impossible.[74] At the same time, these same asymmetric enemies posed little if any threat to joint forces command and control. In this context, winning "hearts and minds" has been, for the last two decades, the information task, *par excellence*.

Unsurprisingly, commanders and information operations practitioners have heavily relied on the integration of the doctrine's newest elements, each of which is essentially a public communication means: PSYOP, PA and CA. This has almost certainly led to the doctrine's tacit reinterpretation. Those with first-hand experience of the irregular wars in Afghanistan and Iraq are especially likely to understand information operations in terms of public relations and strategic communications, despite the doctrine's cybernetic design and its clear adversary focus.

To be sure, public communications have an important role in modern operations. However, large-scale combat operations of the future will almost certainly require commanders at every echelon to fight for superior decision making and better command and control, especially at decisive moments. In light of their dependence on computers, radios, sensors, and other electronic devices, Cold War era specialists answered this very requirement. Their judgment—the basic idea that a positive command and control differential is necessary and achievable, through the integration of various means, to include physical destruction, operations security, military deception, electronic warfare, and others—should once again define our understanding of and approach to information operations.

Notes

1. General William C. Westmoreland, "*Addresses by General W.C. Westmoreland, Chief of Staff, United States Army, Volume IV, 3 July 1969–16 December 1969*," (Washington DC, 1973), 96.

2. Thomas G. Mahnken, *Technology and the American Way of War* (New York: Columbia University Press, 2008), 108.

3. Mahnken, 109.

4. Mahnken, 110.

5. Mahnken, 112.

6. Mahnken, 112.

7. Lloyd Norman, "Westmoreland's J2," *Army* 17 no. 5, May 1967, 24.

8. Norman, 23.

9. R.H. Scherer, "Data Communications and Field Data Information Handling Systems," *Signal* 23, no. 5, January 1969, 8.

10. Scherer, 8.

11. Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 238.

12. Van Creveld, 238.

13. Van Creveld, 238.

14. General William C. Westmoreland, "The Military Uses of Communications-Electronics," *Signal*, August 1969, 73; Van Creveld, 239.

15. Van Creveld, 239.

16. Van Creveld, 239.

17. Westmoreland, "The Military Uses of Communications-Electronics," 30.

18. Ivan Kurnosov, "Development of Radioelectronic Means of Troop Control and Methods of Their Application," *Voyennaya mysl'*, no. 9, September 1964, reprinted in "Selected Readings From Military Thought, 1963–1973," selected and compiled by Joseph D. Douglas Jr. and Amoretta M. Hoeber, *Studies in Communist Affairs*, 5, Part 1 (Washington, DC: US Government Printing Office, 1982), 1.

19. Kurnosov, 1.

20. V. Reznichenko "Modern Weapons and Troop Control," *Soviet Military Review*, December 1978, 11.

21. Reznichenko, 13.

22. V. Kulikov, review of "Idea, Algorithm, Decision," *Soviet Military Review*, April 1974, 56.

23. Lieutenant Colonel Charles J. Davis, "Command Control and Cybernetics," *Army* 13, no. 6, January 1963, 55.

24. Norbert Wiener, "The Human Use of Human Beings: Cybernetics and Society, Da Capo Series in Science" (1954; reprint, Boston: De Capo Series in Science, 1998), 1.

25. Peter Gallison, "The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision," *Critical Inquiry* 21, no.1, Autumn 1994, 234.

26. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 25.

27. Jennifer Light, *From Warfare to Welfare: Defense Intellectuals and Urban Problems in Cold War America* (Baltimore, MD: Johns Hopkins University Press, 2003), 37.

28. Gallison, "The Ontology of the Enemy," 229.

29. Wiener, "The Human Use of Human Beings," 96.

30. Arturo Rosenblueth, Norbert Wiener, and Julian Bigelow, "Behavior, Purpose and Teleology," *Philosophy of Science* 10, no. 1, January 1943, 19.

31. Davis, "Command Control and Cybernetics," 53.

32. Davis, 54.

33. Slava Gerovitch, *From Newspeak to Cyberspeak* (Cambridge, MA: The MIT Press, 2002), 265.

34. Jacob Kipp, *From Foresight to Forecasting: The Russian and Soviet Military Experience* (College Station, TX: Center for Strategic Technology, Texas A&M University, 1988), 178.

35. Kipp, 178.

36. Commander (USN Reserve) Floyd D. Kennedy, "The Evolution of Soviet Thought on 'Warfare in the Fourth Dimension,'" *Naval War College Review*, March–April 1982, 42; David G. Chizum, *Soviet Radioelectronic Combat* (Boulder, CO: Westview Press, 1985), 20–21.

37. Chizum, 3.

38. Chizum, 24.

39. Kennedy, "The Evolution of Soviet Thought on Warfare in the Fourth Dimension," 42.

40. Department of the Army, Field Manual (FM) 100-2-1, *The Soviet Army, Operations and Tactics* (Washington DC: 16 July 1984), 5-81.

41. Chizum, *Soviet Radioelectronic Combat*, 4.

42. Chizum, 9.

43. Chizum 1.

44. Charles F. Smith, "Command, Control and Countermeasures (C3CM)," *Military Review* 63, no. 1, January 1983, 68.

45. Alan D. Campen, Contributing Editor, *The First Information War: the Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Virginia: AFCEA Press, 1992), x.

46. Campen, xiv.

47. Colin Powell and Joseph Perisco, *My American Journey* (New York: Ballantine Books, 2003), 509–510.

48. First Lieutenant (USAF) Gary A. Vincent, "A New Approach to Command and Control: The Cybernetic Design," *Airpower Journal*, Summer 1993, 27.

49. Kathy J. Perry, "The Use of Psychological Operations as a Strategic Tool," Research Project, (Carlisle: US Army War College, April 2000), 7.

50. Alvin Toffler and Heidi Toffler, *War and AntiWar: Survival at the Dawn of the 21st Century* (New York: Little, Brown and Company, 1993), 80.

51. Campen, *The First Information War*, 173.

52. Andrew F. Krepinivich Jr., *The Military-Technical Revolution: A Preliminary Assessment* (Washington DC: Center for Strategic and Budgetary Assessments, 2002): iii.

53. Krepinevich, 8.

54. Krepinevich, 8.

55. Krepinevich, 8.

56. Krepinevich, 8.

57. Krepinevich, 22–23.

58. Krepinevich, 23.

59. Krepinevich, 22.

60. Krepinevich, 22.

61. Alvin Toffler and Heidi Toffler, *War and AntiWar*, 3.

62. Toffler and Toffler, 71.

63. Ian Curtis, "Misinformed About Information War? The Three-Wave Theory is Under Fire," *Defense and Foreign Affairs Strategic Policy*, March 1996, 4.

64. Toffler and Toffler, *War and AntiWar*, 64.

65. Robert J. Bunker, "The Tofflerian Paradox," *Military Review* 75, no. 3, May–June 1995, 99.

66. Bunker, 99.

67. Joint Chiefs of Staff, Joint Publication (JP) 3-13.1, *Joint Doctrine for Command and Control Warfare* (Washington DC: 7 February, 1996): v–vi.

68. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-69, *Concept for Information Operations* (Washington, DC: 1 August 1995).

69. TRADOC Pamphlet 525-69, 4.

70. TRADOC Pamphlet 525-69, 12.

71. TRADOC Pamphlet 525-69, 10.

72. Department of the Army, Field Manual (FM) 100-6, *Information Operations* (Washington DC: August, 1996), 1-3.

73. Department of the Army, FM 100-6, 3-10.

74. Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: First Vintage Books, 2007), 19.

Chapter 2

US Information Operations in Large-Scale Combat Operations: Challenges and Implications for the Future Force

Major Justin B. Gorkowski

Anyone who has participated in a Decisive Action Training Environment (DATE) rotation will be quick to say that assured communications, navigation, and air superiority over the past two decades have spoiled the force. The information environment of future large-scale combat operations (LSCO) will be contested at best. Providers of Information-Related Capabilities (IRCs) will conduct preparatory fires on a multidimensional battlefield months or years ahead of the physical deployment of forces. IRCs will evolve to include all elements that have the ability to penetrate the information domain, shape physical combat activity, and maximize potential for expeditionary operations. Information supremacy will be marked by windows of opportunity, which mandates redundancy through analog or commercial off-the-shelf systems. A revolution in military information affairs in the face of adversarial advances in technology and application will prepare and enable the Department of Defense for the unified application of IRCs to ensure success.

This chapter reflects the study of the current state of information operations in the US Army, adversary information warfare posture, and the anticipated future state of the information environment. These points are applied specifically in consideration of the ability to address major adversaries in future LSCO. Individually, US IRCs perform new and innovative functions every day. They are managed by agile leaders who adapt to the changing information environment and think creatively to develop unprecedented applications for constantly changing technology. However, they largely remain insulated from the other IRCs and thus, the utility of the collective power of information warfare is not maximized. The challenge of integrating capabilities into combined arms warfare is not new for the US Army. Lessons from warfare throughout history serve to inform the US military in terms of preparation for future major combat. Such a challenge will require substantial change from a mindset, doctrinal, and personnel standpoint. The remainder of this chapter will unpack these points.

The first section will address endogenous variables of concern, which are comprised primarily of organizational structure challenges. The following section elaborates on historical examples of similar challenges in the US military. Next, an analysis of adversary information warfare proves indicative of adversary intent in terms of costly signals and commitments.

The next section provides a hypothetical glimpse into the future information environment LSCOs would operate within. Finally, this chapter will conclude with summary implications and recommendations for change needed to address future large-scale combat operations. Ultimately, the challenges the United States faces in terms of the effective employment of information operations in LSCO are familiar—they are structural and consist of close coordination, integration, and realistic training. The US Army has addressed such challenges before and the same solutions apply in this context.

Where Do We Stand? Endogenous Challenges and Limitations

Perceptions of what information operations are and the effects they are intended to achieve vary considerably across the US Army, and even more so across the joint force and interagency world. There are examples of tactics and strategies that have worked well in counterinsurgencies that may not translate to LSCO. Ask five different maneuver battalion or brigade commanders what information operations (IO) are and how IO can help them, and you will get five different answers and a lot of confused looks. This is the state of IO in the US Army today. The most difficult task of an IO practitioner is to demonstrate to the operations officer and commander the ability of IO to be a combat multiplier without the possession of any significant assets or staff. This description may seem harsh, but it represents a reality that is actually much more supportive of IO than just five years ago. This section will outline key aspects of the current doctrine of IO in the US Army and structural challenges with integration and interagency efforts.

A discussion of the role of IO must first begin with a baseline understanding of where IO stands currently as a field. US doctrine defines information operations as the integrated employment of IRCs.[1] IRCs consist of a laundry list of capabilities that have the potential to influence the information environment, such as Cyber Electro-Magnetic Activities (CEMA), Military Information Support Operations (MISO) or psychological operations (PSYOP), civil affairs (CA), Combat Camera (COMCAM), Human Terrain Teams (HTTs), space operations, special technical operations and deception, Soldier and Leader Engagements (SLEs or meetings), and others.[2] It is important to note these are capabilities over which dedicated IO personnel typically have no direct control. Trained IO officers (there are no non-commissioned officers) now reside at the division level and above. The current structure of IO personnel throughout the force serves as a hindrance to the integrated employment of IRCs, as will be made clear throughout this chapter.

Up until 2015, the Army employed trained IO officers at the brigade level to assist with coordinating and employing IRCs. Although challenges regarding access to IRCs existed, dedicated IO officers at the brigade level at least had the ability to request assets and integrate effects. Unfortunately, recent doctrinal changes resulted in retaining trained IO personnel at the division level and above, with CEMA, CA and MISO personnel now falling directly under the operations officer at the brigade level. IRCs at all levels are now the most stovepiped and least integrated doctrinally in the history of the IO functional area. This reality is exacerbated by the adversary, as David Kilcullen's findings highlight below:

> We typically design physical operations first, then craft supporting information operations to explain our actions. This is the reverse of Al Qaeda's approach. For all our professionalism, compared to the enemy's, our public information is an afterthought. In military terms, for Al Qaeda the main effort is information; for us, information is a supporting effort.[3]

The information warfare doctrine of major state-level adversaries increasingly reflects the approach of Al Qaeda mentioned above. Fortunately, some US leaders have empowered IO personnel to task organize in a more integrated fashion to address the current and anticipated future information environment. This was evidenced most recently by the 4th Infantry Division (ID) during their participation in Operation Atlantic Resolve, where the division staff organized into an ad hoc Information Related Capabilities cell to maximize resources and synchronize capabilities.[4] Key IRCs were task organized under a single officer in charge with commensurate rank of other senior division staff officers, which maximized information sharing and unity of control. Unsurprisingly, such task organization by 4th ID was successful. Individually, IRCs are proven to provide valuable effects. However, when IRCs are synchronized, the synergy that develops can be incredibly powerful. There are recent examples in Afghanistan of tactically integrated information operations, such as the delivery of MISO messages transmitted through electronic warfare ground and aerial systems intended to deceive the enemy through his handheld radio receiver. Integration is powerful if properly resourced.

Although it is not reflected so much in doctrine, it is worth noting there is a strong tendency in the US to equate IO with marketing or advertising, especially in counterinsurgency warfare. The "war of the story" and "control of the narrative" are now common phrases in the IO lexicon. The US Army IO qualification course includes blocks of instruction on marketing principles, and training with industry opportunities are typically

associated with marketing or advertising firms. Marketing and advertising are certainly useful as a thought process in many ways, but from a tactical standpoint, it is important to focus on changing behavior rather than attitudes. In LSCO, time will be of the essence, and information operations will need to target specific audiences for behavioral change in order to multiply combat effects. Should an army patrol care if the local population likes them as long as they are not detonating improvised explosive devices (IEDs)? Research beginning in the 1930s demonstrates that, "attitudes are very poor predictors of behavior."[5] Conversely, once behavior changes, attitudes are likely to follow. Retired UK Major General Andrew Mackay and Royal Navy Commander Steve Tatham have written extensively on this topic. In a 2012 report for the Defence Academy of the United Kingdom, they argued the RAND's findings on US information operations in Afghanistan were fundamentally wrong and overly reliant upon marketing and advertising principles.[6] In LSCO, the US Army should be concerned little with the business of advertising. Information operations efforts should instead be focused on influencing what the adversary does or does not do (behavior). In order to effectively target adversary behavior, US IO elements need to perform detailed Target Audience Analysis (TAA) well ahead of LSCO. This point will be expanded upon later.

Finally, another challenge with the current state of IO is scale and interagency coordination. Given the expansiveness and instant nature of the information environment, very little discretion is afforded for the tactical employment of IO. With advances in technology, the gap between the strategic level and the tactical level is narrowed considerably. This results in risk aversion by the US State Department and other interagency partners who seek to control US credibility and the overarching narrative. In the event a tactical need arises for the employment of IO, approval authority is often held at too high a level to achieve prompt effects on the ground. This lag will delay or potentially negate the utility of IO in future LSCO.

As evidenced above, the primary limiting factors in the employment of information operations in future large-scale combat operations are structural. When the need arises and key personnel are empowered by a dynamic commander, the Army has demonstrated the ability to task organize to defeat the threat. However, US doctrine and personnel allocations currently prohibit the ability to maximize utility. These issues are compounded by interagency approval authorities and discretion delegated to the tactical level. As noted in the next section, these types of challenges are not new.

Examples from Yom Kippur: Same Problem, Different Capabilities

What are some historical examples of stovepiping or integration problems in the military? One example is the Yom Kippur War, which was foundational to the establishment of US AirLand Battle doctrine. Two of the most significant lessons of the Yom Kippur War, as noted by the inaugural commander of US Army Training and Doctrine Command (TRADOC) General William DePuy, were the close operational coordination between the air and ground forces and the importance of combined arms teamwork, which required employment in realistic training.[7]

The US has learned many lessons in terms of combined arms maneuver through the nearly two decades of recent conflict. There are two important considerations with regard to the US operations in information environment since 2001: the information environment has evolved and expanded rapidly, thereby generating new means for warfare; and US operations within the information environment have been relatively uncontested. As a result, the US has not been forced to learn the hard lessons on how to employ information operations as an element of combined arms maneuver. So how does the United States adapt to defeat the enemy in a contested information environment? A revolution in military information affairs is needed.

A Look at the Adversarial Approach: Exogenous Concerns

Major adversaries have wasted no time exploiting the information environment and signaling intent. Russia's doctrine of New Generation Warfare is primarily a strategy of influence.[8] The objective of Russian information warfare is to control information in whatever form it takes—information is the object of operations, not the platform through which it flows.[9] Similarly, China's goal with information warfare is to secure information dominance through technology and psychological operations.[10] With the control of information, one can control what the adversary hears or sees in the information domain, which results in ambiguity increasing or decreasing in support of kinetic operations. In other words, control of information can lead an adversary to think what they are hearing and seeing is truth when it may just be part of a broader deception or manipulation. Other than the mindset, which holds information as the object of operations, adversary information warfare differs from that of the United States in a few important ways: structural integration, phases of employment, and data collection. These points are summarized below.

Structural Integration

The Russian model for information warfare is comprehensive and holistic. All of what the United States considers IRCs are unified under the Russian structure, which falls under the leadership of the Russian General Staff.[11] Propaganda, deception, cyber, political, and economic warfare capabilities are all part of unified information operations. The Russian incursion into Georgia in 2008 was the country's first experiment with integrated information and kinetic warfare. Specific deficiencies were identified following major operations that fell into two categories: information-technical and information-psychological.[12] This perceived shortfall led to calls for specific "information troops":

> The personnel of the Information Troops should be composed of diplomats, experts, journalists, writers, publicists, translators, operators, communications personnel, web designers, hackers, and others. . . . To construct information countermeasures, it is necessary to develop a center for the determination of critically important information entities of the enemy, including how to eliminate them physically, and how to conduct electronic warfare, psychological warfare, systemic counterpropaganda, and net operations to include hacker training.[13]

Russian incursion into Crimea in March 2014 presented another opportunity to test information warfare. In this case, Russia established physical control over the telecommunications infrastructure to isolate Crimea from news from the outside world.[14] Russian special forces were able to simultaneously interface kinetic and information operations to manipulate information received by internal and external target audiences. In the case of Crimea, this resulted in confusion and a lack of significant escalation or hostile action. The employment of information warfare in Crimea was viewed much more favorably.

The Grey Zone and Phases of Employment

Adversaries the US military are most likely to face in LSCO do not distinguish between peacetime and wartime from an information warfare standpoint. Efforts are ongoing to seize the initiative in anticipation of future conflict. This point is solidified below in an excerpt from 2010 Russian military doctrine:

> Features of modern military conflicts include the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and,

subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force.[15]

The Russian concept of information operations, or more appropriately information warfare, applies to times of peace and conflict. The information realm is one in which adversaries are comfortable operating without significant fear of reprisal or overt US military response. China operates along the same lines, as indicated by a publication by the Chinese Academy of Military Science below:

> It is necessary in peacetime to undertake information warfare in the political, economic, technical, and military realms, as only then can one scientifically establish operational plans, appropriately calculate gains and losses in a conflict, appropriately control the level of attack, precisely strike predetermined targets, and seek the best strategic interest and long-term benefit.[16]

There are no conflict specific rules of engagement; Russian and Chinese information operations preparatory fires have already commenced. Unfortunately, such operations in the grey zone fall below the threshold of overt US military response.[17] Adversaries continue to exploit this reality.

Data Collection

A critical component of grey zone operations for adversaries includes data collection. This is done in a number of ways, but significant effort is attributed to social media. US Soldiers participating in Operation Atlantic Resolve in 2015 were targeted in this regard. Social media data was collected on individual officers visiting Kiev and mixed with allegations of child rape on Russian-backed media outlets.[18] Russia has demonstrated effectiveness in mixing seemingly reliable information with credible sources to disseminate fake news. Western reliance on social media and cellular communications present a critical vulnerability. The implications of examples like this on US participation in LSCO are immense and well summarized by Keil Giles:

> In time of crisis, if the defense forces of a frontline state decided to mobilize in response to a direct and immediate threat from Russia, it might find that its personnel—and government officials more broadly—receive apparently trustworthy instructions to remain at home and offer no resistance.[19]

Russian intelligence collection on data that can be used to target individuals or groups through the information environment in conjunction with other operations is well underway. The same can be safely assumed

for China with one example being their massive data breach of the US Office of Personnel Management (OPM).[20]

In summary, the exogenous challenges to information operations by key adversaries outlined above should inform how the US approaches information operations in LSCO. The information environment for such a conflict is already being exploited for adversarial advantage. The next section outlines a hypothetical scenario where an adversary initiates LSCO while maximizing the utility of information warfare.

Setting the Stage: A Hypothetical Glimpse of the Information Environment in LSCO

The information environment for LSCO includes the environment currently being exploited by adversaries. Such an environment is much more representative of what Clausewitz considers total war, comprising at least two elements of the trinity. Primary information warfare objectives will focus on data collection and manipulation with secondary efforts focused on contextual, phased dissemination in conjunction with supported operations. Effects will include deception, diversion, character assassination, and economic shock and will seek to widen cleavages and invoke emotion. Political active measures and economic warfare will be of primary concern to adversaries. Active measures will be employed to influence political outcomes.[21] Adversaries will pursue character assassination through emotion invoking or volatile issues such as claims of sexual assault, race, or sex scandals. Economically, adversaries manipulate the transportation infrastructure by imposing a minor tax on the system to slow the distribution of goods while activating sleeper cell devices such as ZTE phones to passively or actively collect insider information.[22] Russian hacktivists and patronage networks tapped by the Russian Business Network (RBN) are activated to add complexity and generate revenue.[23] As chaos ensues under the radar, all channels for information dissemination to specific target audiences indicate normal operations. Meanwhile, the adversary military mobilizes under a specifically woven camouflage of information concealment.

Militarily, US regional defense forces are informed through quasi-official channels to remain in place. Adversary hackers target USAA and empty Soldiers' bank accounts as they begin to mobilize. The enemy dumps large quantities of fake news on WikiLeaks and other outlets to mislead and deceive US military decision makers while simultaneously forcing US officials to disprove the allegations. Tactical Electro-Magnetic Pulse devices are strategically employed around the globe and Position-

ing, Navigation, and Timing (PNT) devices are knocked out in predetermined sequence. Once the US military finally begins to mobilize, initiative has already been seized and the US government has to operate within the constraints of democratic and institutional norms.

The crude vignette outlined above is perhaps not much of a departure from reality. If a major adversary initiates LSCO, they would be hard pressed to avoid exploiting some of the vulnerabilities presented here. While actual events in LSCO would be much more nuanced and dynamic, the vignette is helpful in framing implications and recommendations.

Summary Implications and Recommendations

Given the international status quo and stabilizing factors such as international institutions, the US is not likely to initiate major war. Therefore, US participation in LSCO will likely be reactive and consist of an initial loss of ally held terrain. In such a scenario, the US has already come to terms with the fact that reactive mobilization will prove timely and costly.[24] Critiques of US forces positioned in Eastern Europe have been referred to as "speedbumps" or "tripwires," but as alluded to by Thomas Schelling during the Cold War, these forces are in position as a deterrent, not to defend Europe.[25] Such positioning serves as a costly signal to demonstrate to adversaries that any aggression implicating these forces means the United States is automatically committed to the conflict. The implications and recommendations outlined below are in summarized in terms of deterrence and compellence.

Deterrence

The positioning of troops in Eastern Europe serves as a useful example of a costly signal. The same logic should be applied to the information environment for future LSCO. Costly information signals need to be employed in the information environment as tripwires that automatically commit the US to military action. If such costly signals are not clearly communicated, adversaries will continue to manipulate the information environment in their favor to maximize advantage during the outbreak of major conflict. This is clearly not just an Army problem, but the Army must advocate as a part of strategic change. The US has struggled considerably in the political realm to establish regulations for fear of imposing on private corporations or industry and damaging the domestic economy. Similarly, international regulations remain lax and clouded in uncertainty. Meanwhile, state aggressors like Russia and China exploit the information environment to their benefit. This must change for deterrence in the in-

formation environment to take root. Recommendations for addressing the challenges of deterring adversaries through information warfare in LSCO are listed below:

• *Emplace Costly Signals.* Major adversaries are not going to change current behavior unless the United States clearly communicates costly signals. The United States and allies must emplace "tripwires" in the information environment that credibly commit the United States to action if terms are violated. A lack of costly signals will result in continued exploitation of the information environment and significant disadvantage in the event of LSCO.

• *Institutionalize Western Information Operations.* The United States needs to lead the development, manning, and exercise of international institutions, such as the NATO Strategic Communications Center of Excellence in Latvia with the goal of developing practices and sharing lessons learned. Meaningful participation by the United States again demonstrates a credible commitment to state aggressors. Such institutions should be heavily involved in regional exercises.

• *Embrace the Grey Zone.* The distinction between peace and conflict is blurred. The United States is currently limited in the types of authorized operations during times of "peace." The adversary is exploiting this fact. Phase zero began long ago and this will require a certain amount of catching up on the part of the United States In March 2016, General Joseph Dunford commented that most combatant commanders believe the adversary is operating in Phase 2 or 2.5 where they are seizing the initiative. In order for the United States to set conditions for successful shaping operations and regain the initiative for LSCO, significant TAA is needed. Such TAA should consist of all elements of adversary national power, to include soft power. Perhaps the Pentagon should reconsider programs similar to Project Camelot to conduct detailed ethnographic research.[26] Such efforts are intelligence heavy and should be driven by information operations objectives.

Compellence

Once deterrence fails, the US Army needs the assets and resources to compel adversary action. In May 2018, a joint group of senior ranking military officers met at Quantico to discuss the challenges of integrating multi-domain operations. The key theme reported out of the meeting was regarding challenges due to integration across domains.[27] There were many similarities and even graphical references to AirLand Battle. A key point that needs clarification with the current concept of Multi-Domain

Battle (MDB) is how information is viewed and operationalized. The Russians would view information as a stand-alone domain, through which capabilities like CEMA operate. The platforms or IRCs operate to influence the object of operations, which is information. The challenges outlined in MDB concept released in December 2017 are indicative of the challenges involved with the US operationalization of information warfare.[28] Integration of capabilities across domains with precision and maximum utility is incredibly difficult, especially when faced with a peer or superior adversary. In terms of information operations, the first step toward maximizing utility from a compellence standpoint is to clearly define and unify the concept of information operations across the joint force. Recommendations for addressing the challenges of compelling adversaries through information warfare in LSCO are listed below:

• *Commission a Study.* This may seem cliché, but necessary. Individual services and agencies have developed their own definitions of information operations. The services are not even in agreement on the phrase (i.e. information operations vs. information warfare). A comprehensive study should include experts from the Department of Defense, interagency, and academia. The study should consider the current information environment, capabilities and doctrine of the United States and allies, adversary capabilities and doctrine, and anticipated future threats. The findings of the study should inform key decision makers of changes needed to address emerging information operations challenges.[29]

• *Empower the Information Dominance Force.* Considerable doctrine and personnel changes are needed within the Information Dominance career field to maximize utility in LSCO. Information Dominance professionals need to be "cross pollinated" to reduce barriers to integration and enhance knowledge of synergistic effects. Opportunities for upward mobility and proponency at the highest levels of command are needed effect change that matters. Field grade information operations officers and opportunities for non-commissioned Information Dominance integrators are needed at the tactical level. Doctrine and qualification courses need to reflect combat requirements for adversarial behavioral change. The creation of comprehensive Information Warfare brigades comprised of all IRCs (including economic, political and legal advisors) that can be task organized to support all levels of command may help address these challenges.

• *Enhance Joint and Interagency Partnerships.* In order to maximize utility, joint and interagency partners need to operate from the same playbook. If an adversary applies information warfare in a specific area, the

entire force needs to equally understand the potential implications. In the information environment, the gap between the strategic and tactical levels is minimized. LSCO will require strategic assets and discretion at the tactical level in near real time. This will only happen if structural changes are made to place information warfare personnel strategically throughout the joint and interagency structure in positions where decisions are made.

• *Build Redundant and Analog Information Capabilities.* Information dissemination in contested information environments, as expected in LSCO, will be vulnerable to constant disruption and manipulation by the adversary. Periods of digital information blackout will be sporadic. Information warfare intent must be clearly communicated and empowered at the lowest levels for effective employment. Redundant systems should be in place in the event of information failure.

In the end, we come full circle back to the lessons learned by General DePuy and his staff at TRADOC after the Yom Kippur War that led to the creation of the National Training Center. There is no substitute for intense, realistic combined arms training. In order for this type of training to be successful in the current information environment, all non-lethal enablers or IRCs need to have the proper authority and be placed appropriately throughout the formation. The new Information Dominance category needs proponency with a voice and with options for upward mobility in all of the respective IRCs. Such personnel should be placed at all levels of command and include noncommissioned officers.

We are already operating in the information environment in which future large-scale combat operations will occur. The challenges presented in the information environment have a largely structural solution. The individual IRCs in the US military are incredible and improving every day with advances in technology. The US military should approach this challenge from a functional standpoint to flatten stovepipes that have emerged through advances in technology. Empowering leaders who can bridge the gaps that currently exist between the IRCs through a restructuring of the US military approach to information warfare is the only way the increasingly powerful capabilities of cyber, electronic warfare, deception and collective information operations can seamlessly merge with kinetic operations to defeat major adversaries in LSCO. Significant opportunity exists for the US to regain the initiative.

Notes

1. See Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: 27 November 2012) and Department of the Army Field Manual 3-13, *Information Operations* (Washington, D.C.: December 2016) for a more detailed definition.

2. Department of the Army, FM 3-13, 1-3.

3. Andrew Mackay and Steve Tatham, *Behavioral Conflict: Why Understanding People and Their Motivations Will Prove Decisive in Future Conflict* (Essex: Military Studies Press, 2011), 135.

4. Matthew Sheiffer, "US Army Information Operations and Cyber-Electromagnetic Activities: Lessons from Atlantic Resolve," 19 March 2018, accessed 2 June 2018, http://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/Army-Info-Ops/.

5. Andrew Mackay, Steve Tatham, and Lee Rowland, "The Effectiveness of US Military Information Operations in Afghanistan 2001–2010: Why RAND Missed the Point," Defence Academy of the United Kingdom, Central Asia Series, 2012, 5.

6. Mackay, Tatham, and Rowland, i.

7. Saul Bronfeld, "Fighting Outnumbered: The Impact of the Yom Kippur War on the US Army," *The Journal of Military History* 71, no 2, (April 2007): 477.

8. Center for Strategic and International Studies, "The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe," October 2016, accessed 2 June 2018, https://www.csis.org/analysis/kremlin-playbook.

9. Keir Giles, "The Next Phase of Russian Information Warfare," NATO Strategic Communications Center of Excellence, 4, accessed 2 June 2018, https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

10. Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," The Heritage Foundation, 11 July 11 2013, accessed 2 June 2018, https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

11. Oleg Odnokolenko, "Shoygu Orders Information Troops to Take Offensive," *Nezavisimaya Gazeta Online*, 27 February 2017, accessed 2 June 2018, http://www.ng.ru/armies/2017-02-27/2_6936_shoigu.html.

12. Keir Giles, "Information Troops—A Russian Cyber Command?" 3rd International Conference on Cyber Conflict, 2011, accessed 2 June 2018, https://pdfs.semanticscholar.org/7b93/b0b24c10aa0e009b41059e86de054df1711f.pdf.

13. Giles, "Information Troops," 52.

14. Giles, "The Next Phase of Russian Information Warfare," 12.

15. "The Military Doctrine of the Russian Federation," 5 February 2010, accessed 2 June 2018, https://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

16. Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge."

17. Paul Scharre, "American Strategy and the Six Phases of Grief," *War on the Rocks*, 6 October 2016, accessed 2 June 2018, https://warontherocks.com/2016/10/american-strategy-and-the-six-phases-of-grief/.

18. Giles, "The Next Phase of Russian Information Warfare," 14.

19. Giles, 14.

20. Ellen Nakashima, "Chinese breach data of 4 million federal workers," *The Washington Post*, 4 June 2015, accessed 2 June 2018, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html?noredirect=on&utm_term=.e943c37fe800.

21. Central Intelligence Agency, "Soviet Active Measures: Forgery, Disinformation, Political Operations," Special Report No. 88, October 1981, accessed 2 June 2018, https://www.cia.gov/library/readingroom/docs/CIA-RDP-84B00049R001303150031-0.pdf.

22. Sherisse Pham, "US hits major Chinese tech firm with export ban," CNN, 17 April 2018, accessed 2 June 2018, http://money.cnn.com/2018/04/17/technology/zte-china-us-phones-ban/index.html.

23. Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *Journal of Slavic Military Studies*, 27, 2014, 101–130.

24. Sydney Freedberg Jr., "Generals Worry US May Lose In Start Of Next War: Is Multi-Domain The Answer?" *Breaking Defense*, 14 May 2018, accessed 2 June 2018, https://breakingdefense.com/2018/05/generals-worry-us-may-lose-in-start-of-next-war-is-multi-domain-the-answer/.

25. Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 47.

26. George Packer, "Knowing the Enemy: Can social scientists redefine the war on terror?" *The New Yorker*, 18 December 2006, accessed 2 June 2018, https://www.newyorker.com/magazine/2006/12/18/knowing-the-enemy.

27. Freedberg, "Generals Worry Us May Lose In Start of Next War."

28. US Army Training and Doctrine Command, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century, 2025–2040," Version 1.0, December 2017, accessed 2 June 2018, http://www.tradoc.army.mil/multidomainbattle/docs/MDB_Evolutionfor21st.pdf.

29. Such a study should at a minimum include Keir Giles, Heather Conley, Andrew Mackay, Steve Tatham, and Maxell Thibodeaux.

Chapter 3
The Fog of Russian Information Warfare

Lionel M. Beehner, Colonel Liam S. Collins, and Robert T. Person

"This is an arms race," Facebook Chief Executive Officer Mark Zuckerberg told a recent congressional panel in reference to the Russian Federation's use of social media to conduct information warfare. "They're going to keep getting better."[1] The tools and tactics of Russian information warfare may have changed over the decades, but as many analysts have noted, the ends remain largely unchanged since Soviet times: to complicate, contain, and constrain the projection of US strategic power and those of its allies, predominantly in Eurasia but also in the Middle East. It is an entirely rational way of shaping the strategic environment to gain advantage, given the quantitative and qualitative asymmetries between Russia and the West in conventional capabilities.

With the US Army shifting its doctrinal focus from counterinsurgency to large-scale combat operations, peer and near-peer competitors such as China, Iran, and Russia are taking on renewed importance.[2] But that does not necessarily imply a complete doctrinal shift toward large-scale conventional operations, given all the types of warfare these states prefer to wage. After all, so-called "contactless war," as the Russians define it, is meant to negate their military disadvantage by avoiding any direct contact with Western forces, whether by demonstrating fire discipline or deploying "little green men" in places like Crimea.[3] Russia has shown a remarkable ability and willingness, with fairly straightforward means, to disrupt democratic institutions, undermine social cohesion, and sow confusion, doubt, and distrust among Western allies and their publics. Social media has only accelerated the pace of information warfare (IW) advancement.

We should be clear by what is meant by Russian information warfare, or *informatsionnaya voyna*. Information warfare is not simply a tool to achieve some kind of limited tactical objective or advantage during wartime, typically in the initial phase of hostilities. Rather, information warfare should be considered more broadly. Calculated and systematic, it consists of operations aimed at degrading the enemy's ability to control the information space, deny it the technical capability to retaliate via cyberspace means, and defend a narrative of Russian nationalism to glorify its role on the world stage—a manipulative form of Russian "soft power." Russian information warfare comprises a bounty of tactical innovations, from traditional psychological operations (psy-ops) and strategic com-

munications aimed at controlling the narrative, to the sophisticated deployment of decentralized trolls and bots across social media and other online platforms.[4]

Russian information warfare—*informatsionnaya voyna*—consists of three pillars. First, and most benignly, it aims to put the best spin it can on ordinary news. It does this through state-controlled outlets like RT (formerly "Russia Today"), Russian-language radio ("Sputnik"), as well as through television outlets that cater to the Russian-speaking population of the former Soviet states. This spin generally paints Russia as a viable and preferred alternative and counter to US greed and aggression."[5] Second, it uses disinformation to create enough ambiguity to confuse people, both at home and abroad, about its current operations, whether in Ukraine, Syria, or elsewhere, all with the aim of providing a decoy and contributing to the proverbial "fog of war." Third, it outright lies when given true information and claims it is falsified. This last strategy has several objectives: to degrade trust in institutions across the world; push populations currently undergoing conflict to simply accept the status quo of the conflict and not push for resolution; and finally, it prevents countries in its desired sphere of "privileged interest" from Western alliances like NATO by keeping these areas in perpetual conflict.

Interestingly, while Western technology firms point to an arms race with peer competitors like the Russian Federation and the People's Republic of China, the US government does not consider itself at war. This naivety is a strategic mistake, we argue. In this chapter, we examine how Russian information warfare operates and how it should be conceptualized at the strategic level. How does information operations (IO) fit into Russia's larger strategic aims? What are its primary methods? And finally, and perhaps most importantly, how can the US military effectively combat Russian information warfare, while staying true to its values and simultaneously preventing conflict escalation? In this chapter, we advance three central arguments:

- First, Russia's leadership does not apply information warfare solely to support its military objectives—as a way to soften up the enemy or prep the battlefield, as it were—but rather vice versa. Its military operations in places like Ukraine or Syria are often ancillary to Russia's more immediate strategic objective: to challenge US interests wherever possible and undermine America's ability to advance unhindered its own strategic objectives. As such, it can be considered a form of post-Cold War strategic balancing by Moscow that involves political, economic, cyberspace, and—most formidably—information means to contain and constrain US

activities globally. In this sense, IW should not be seen as simply a tool in Russia's *military* toolkit. While Russian IW has certainly been used as part of military operations, it is often applied in pursuit of Russian political objectives where military objectives may be absent. Thus, when observers see evidence of Russian IW, they should not immediately jump to the conclusion that they are part of a military strategy to formally seize more land in Ukraine's east or send a column of tanks into the Baltics. Regarding Russia's IW efforts, the ends are to challenge American interests and undermine the foundations of Western democratic institutions; by sowing uncertainty, discord, and division in the United States and its allies, IW tactics are a particularly cheap, ambiguous, and effective means of achieving those strategic ends. To the degree that information warfare goes hand in hand with Russian conventional military operations, recent experience demonstrates that the latter are in some respect sideshows to the former, not the other way around.

• Second, while information warfare is frequently applied for non-military political ends, Russia nonetheless considers itself at war with the West and brings such a mentality to its operations. Moscow thus conducts information warfare primarily preemptively to weaken its enemy—the United States and Europe. Information warfare was formally incorporated into Russian military doctrine in 2010, and dates further back to the height of the Cold War, but it was been exponentially expanded on since. To date, Russia has seen itself as able to achieve "information dominance" —that is, the ability to penetrate the American information environment, from planting stories in the media to hacking the emails of politicians and their operatives, and influence political outcomes.[6]

• Third, when it comes to Russian aggression in the information realm, we are at war. Though it may be "political warfare," to borrow George Kennan's term from a 1948 Policy Planning Staff memo, it is warfare nonetheless.[7] To counteract Russian malicious activity, one must "fight fire with fire." US conventional deterrence in the region has primarily consisted of stationing several battalions in NATO partners like Poland and the Baltics. Yet, a recent RAND report found that Russia would overrun NATO forces in a matter of hours.[8] The imbalance is even more severe in the informational realm: there is neither a sufficient deterrent to prevent Russian IW attacks, nor a punitive mechanism to enact retaliatory measures beyond issuing statements condemning such acts. We recognize that attribution is an issue in this space, as is the risk of conflict escalation. However, the current defensive position of the United States is not working. To quote one congressman, "[W]hy not go on the offense to release information expos-

ing corruption at the Kremlin?"[9] Without looser rules of engagement and a more offensive strategy, we can expect Russia and its agents to continue its concerted information operations unabated as the United States continues to cede the strategic initiative in the information environment.

This chapter proceeds as follows: First we provide some background of Russian IW, define several key concepts, and identify the main methods Russia uses and the challenges they pose. Next, we lay out the larger strategic aims of Russian IW, both against the West and against Ukraine and other former Soviet states. Then we detail its IW methods by examining the case study of Ukraine. We conclude by outlining a list of recommendations for the US military to effectively combat Russia's IW efforts.

Information Operations 101

Clausewitz correctly noted that the nature of warfare never changes, only its character. He would have recognized the character of information warfare as a distinct and effective form of warfare to accomplish one's political ends, given that an enemy's center of gravity is shifting. The United States' greatest strength is paradoxically also its greatest weakness: that is, our freedom of speech and press. Here the Russians are practicing a playbook straight out of Clausewitz: attack the enemy where they are *most* vulnerable. The US military defines information operations as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[10] Further, it defines information warfare as "a threat's orchestrated use of information activities (such as cyberspace operations, electronic warfare, and psychological operations) to gain an advantage in the information environment." In other words, IO refers to friendly actions in the information environment, while IW is used to describe threat-based activities.

In keeping with our argument about Russian IW as a form of political warfare, it is important to note that the definition above is overly restrictive in defining information warfare as residing strictly within the confines of military operations. Thus, we find it useful to employ a "holistic concept [of information warfare] that includes computer network operations, electronic warfare, psychological operations, and information operations."[11] Information warfare—sometimes called "influence operations"—refer broadly to the practice of collecting information about an enemy as well as the dissemination of disinformation and propaganda to seek an advantage over one's adversary, whether in peacetime or wartime.

Russian information warfare is carried out through five main methods, ranging from psychological to technical: the manipulation of information (fake news), espionage (intelligence), political interference, military deception (plausible deniability), and cyberspace-based capabilities (social media). The latter is the only item that is really new and innovative, as it allows for increased speed and allows for further distance. We outline these methods below.

First, Russia has mastered the use of fake news and other disinformation to confuse or persuade media consumers, both in Russia and the West. The purpose of this effort is to erode public support and confidence in Western democratic institutions, to create and amplify public and a political discord, to create confusion in order to delay Western decision-makers at the highest levels, and to intensify the security competition in areas of strategic importance to both the West and to Russia. This is especially true in Eastern Europe and the South Caucasus along the fault line between NATO and the countries that once orbited within the Soviet Union's sphere of influence: the Baltic states, Georgia, and Ukraine. Intensifying the competition serves to rattle Russia's adversaries, provoke them, and influence their risk-averse publics to disapprove of taking any kind of serious retaliatory measures. Another byproduct of this use of IW is to support both directly and indirectly anti-establishment groups, parties, and politicians in the West—many of them right-wing or hyper-nationalist—as a way to provide them with a veneer of legitimacy and disrupt the democratic process. "Russia's new propaganda is not now about selling a particular worldview," as Alexei Levinson argues. "It is about trying to distort information flows and fuel nervousness among European audiences."[12]

Second, Russian IW includes the work of traditional Cold War-style espionage, like stealing compromising materials and information on one's enemy, known in Russian as *kompromat*.[13] During the Soviet era, this kind of information warfare was referred to as "reflexive control," a theory with deep roots in the Soviet Ministry of Defense's research into psychology and cybernetics that mapped how enemies formed decisions and framed problems.[14] "In the context of warfare," as Maria Snegovaya notes, "the actor that is most capable of predicting and mimicking the reasoning and actions of its opponent has the highest probability of success."[15]

During the Cold War, the primary foot soldiers on this front were KGB intelligence officers, including a young KGB officer in Dresden by the name of Vladimir Putin. Today Russia relies on "information troops," who act as guns for hire in the propaganda realm—contractors, former criminals, and other cyberwarfare actors and middlemen.[16] They are kept at

arm's length from Moscow, to provide the Kremlin with plausible deniability if caught. The aim of these mercenaries is manifold: to disrupt the enemy's telecommunications or data-storage systems; to interfere in and undermine democratic elections in the West, whether by releasing sensitive information, trolling, posting fake news, or other tactics it deems will undermine democracy.

Meddling in foreign elections is not a new tactic. Nor is it a technique unique to Russia or its Soviet predecessor. According to Dov Levin, "Between 1946 and 2000, the United States and the USSR/Russia intervened [to manipulate foreign elections] 117 times, or, put another way, in about *one of every nine* competitive national-level executive elections during this period."[17] What has changed, however, is the technological sophistication, the use of proxies operating on the behalf of nation states, and the ability to leverage the speed of social media. In February 2017, for example, the special prosecutor Robert Mueller charged thirteen Russians and three Russian companies for interfering in the 2016 US presidential election. Among the companies charged was Internet Research Agency, a "Russian troll farm," with the "strategic goal to sow discord in the US political system."[18] In his book, *War in 140 Characters*, David Patrikarakos profiles entire office buildings in Siberia devoted to creating fake news stories to influence voter behavior in Western elections.[19]

The fourth component of Russia's IW is to add to the fog of war and deny the presence of Russian military forces—specifically its use of *spetsnaz* forces in places like Ukraine. This is to distract and obfuscate the existence of an extensive military campaign—what the Soviets used to call *maskirovka*—that might trigger a more robust Western response or worse a backlash at home were the full facts of the operations, including death tolls, to be made public.[20] The Russian government always denies any use of this kind of warfare and instead attributes these attacks to Russian "patriots" operating on their own behalf, with no guidance from Moscow. This kind of disinformation campaign is hardly the work of a decentralized network of pro-Russia grassroots activists improvising on their own but rather is a heavily-structured, national-level effort to facilitate the accomplishment of Russia's strategic objectives. According to former KGB defector, Ion Mihai, this kind of campaign has three prongs: deny involvement, minimize damage, and if truth comes out, blame it on one's enemies.[21]

Finally, in addition to information brigades, election meddling, and deception, Russia employs digital technologies to influence social media and add greater speed and sophistication to its IW campaigns. This in-

cludes, as Keir Giles notes, "a complex blend of hacking, public disclosures of private emails, and use of bots, trolls, and targeted advertising on social media designed to interfere in political processes and heighten societal tensions."[22] Malicious actors can harvest the personal data of unsuspecting users of social media such as browsing history and consumer spending data, which allows them to target groups and individuals by their political views, their income bracket, and their location. They can then plant contradictory messages in news stories that already expose ideological fault lines. A case in point was Russia-linked bots and trolls pushing divisive stories and hashtags on social media that fueled the National Football League national anthem controversy. Russian hackers also plant false reports in mainstream media outlets. In May 2017, Qatari state media published false remarks made by the emir of Qatar praising Iran, creating an uproar among its Gulf neighbors.[23]

Russian Objectives

This section examines Russian objectives and how IW fits into Moscow's larger strategic aims. Russia is often said to be determined to undermine democracy as an end, and to rewrite the rules of the international order. On this point, Russia is actually quite agnostic to the normative value placed on democracy or liberalism. If the United States were a totalitarian dictatorship marching its forces across the globe, Russia might surmise that playing to people's liberal side might benefit its ability to resist American domination. Russia, in this role, is playing the foil to the United States. In this respect, Russia's grand strategy is non-ideological in its motivation: its target is not democratic institutions per se, rather the target is the political institutions of an adversarial state. That those institutions happen to be democratic is—from an ideological standpoint—immaterial. But from a practical standpoint, the openness of liberal democratic institutions makes them more vulnerable to attack.

What many Western audiences fail to appreciate is the fact that Russia believes itself to be fighting IO fire with IW fire. Moscow's narrative of the 2003 Rose Revolution in Georgia, the 2005 Orange Revolution and 2014 Maidan Revolution in Ukraine, and the 2011-2012 mass protests in Russia is one of a West intent on interfering in its own elections those of countries where Moscow has strong interests. Thus, the Kremlin's view is that its own schemes are simply tit for tat, a game of cat and mouse played against the world's dominant superpower. In seeking to challenge, constrain, and contain American interests, Russia seeks a more multipolar world where it is accorded a seat among the great powers beyond that which it already enjoys with a permanent veto-wielding Security Council position. In Mos-

cow's vision of a multipolar world, great powers like Russia should have a right to spheres of privileged interest, and a free hand to pursue their interests within their sphere unimpeded. The only way to achieve such a world is to roll back American influence. It should also be said that Russia is also a declining economic power playing a weak hand—politically, economically, and militarily. To counter American interests, it relies on IW as a cost-effective, less risky means of warfare.

But this logic requires unpacking. First, Russian information warfare is often treated as just one part of its larger military strategy, which includes a number of other uses of force. However, this diminishes IW's significance, and treats it as just one of several non-kinetic means—a basket of options sometimes referred to as "new generation warfare"—Russia employs in conjunction with kinetic means in pursuit of military objectives.[24] But as argued previously, Russia's objectives are often political in nature rather than military. In fact, IW in pursuit of political ends is appealing for its low cost, low risk, and its relative simplicity. Russia fancies itself as the "great disrupter," to disrupt requires no further end goal than the mere process of destabilizing Western democracy—including its norms, procedures, institutions. Sowing the seeds of chaos is, often times, the primary objective. To be sure, one might argue this is part of a grand design to tilt the rules of the game in its favor by throwing out any rulebook. As Edward Lucas and Ben Nimmo write, "Russia's approach, unlike Nazi Germany's ethnic and ideological one, is deeply nihilistic."[25] Yet it should be emphasized that nihilism is not the ends but rather the means. The ends is to contain and constrain American influence across the globe. When it comes to the bounds of acceptable behavior to achieve this ends, Russia will not follow any rules. As noted in the *Tallinn Manual 2.0* on cyberwarfare, "The Russians are masters at playing the 'gray area' in the law, as they know that this will make it difficult to claim they are violating international law and justifying responses such as countermeasures."[26]

Conceptually speaking, Russia's IW campaign is seen by many Westerners as defensive and in line with what Russia did during the Cold War. But Russia's information warfare activities should be seen as offensive, given that a large part of the effectiveness of IW as a means is its element of surprise. To reiterate, Russia considers itself to be "at war" (or more precisely, "at political war") with the West, yet the West does not consider itself "at war" with Russia. A popular theory among neorealists known as "offense-defense theory" offers insights into the challenge at hand. The theory posits that in cases where the offensive measures enhance a state's security more efficiently than defensive measures, and where a state's

intentions—whether offensive or defensive—are indistinguishable, then the threat of war and instability is greater.[27] The logic is that this kind of setting favors a first-mover advantage and allows for preemptive attacks. This principle also applies to the use of information warfare. There is an element of surprise built in, as well as one of asymmetry. These operations are offensive—even if non-kinetic—by design. According to Maria Snegovaya, "On the tactical level, information warfare allows Russia to achieve surprise in the time or manner of an attack. Russia thereby gains time and efficiency against the enemy's ground forces . . . Informational cover provides more flexibility and efficiency to the military, as well as improves speed of maneuverability and the speed of battlefield responses."[28]

Nonetheless, part of the confusion (and thus the utility from the Russian perspective) of IW is that it can be applied to political ends simultaneously with military ends. In such contexts it can be difficult to determine a priori what the objectives of some information operations are. This is the situation that we find in Ukraine, where political and military objectives are both part of the conflict's logic. It should be stated that Russia's strategy in Ukraine is complicated yet also haphazard. The objective of Russia's military operations in Ukraine *is not* simply to acquire territory—if it wanted to, Russia could have easily annexed militarily the Donbas, the conflict zone in eastern Ukraine, by now—but rather to keep Ukraine down, sow confusion among its public, and prevent Ukraine from joining Western institutions. Russia seeks to undermine the foundational principles of the very institutions that Ukraine seeks to join. In this regard, IW does not serve its military goals of controlling or annexing territory, but rather the other way around: *its military strategy supports its IW*. Ukraine in this regard is just one piece of Russia's larger grand puzzle—an important piece, to be sure, given their close historical ties. Russian military operations in Ukraine are but one component to weaken the West and by extension make the world more multipolar.

IW at the Tactical Level in Ukraine

Russia's information warfare in Ukraine dates back decades, but during the most recent campaign it began in earnest around the time of the Maidan Revolution in November 2013. Russia employed IW against Ukrainian institutions with several objectives in mind: to undermine support for the protesters and pro-western factions in Ukraine, to elicit fear among Ukraine's Russian-speaking and pro-Russian populations in its east and south, and to deny facts on the ground during operations to seize Crimea and interfere in the war in Ukraine's east. To accomplish these

objectives, Russia has employed a number of IW tactics, often in combination with cyber warfare, to influence enemy combatants, local populations, and allies.

First and foremost, the Kremlin sought to control the narrative in Ukraine through a number of efforts targeted at fence-sitters in the region. These efforts include referring to Ukraine in its media or press releases as a "failed" or "fascist" state; releasing forged documents from RAND corporation or the Ukrainian military to paint the latter as corrupt and the former as conspiratorial; citing hoax experts to push fake narratives; manipulating the titles of articles it publishes; amplifying the threat of Europe's disintegration and warning of the West's declining support for Ukraine (so-called "Ukraine fatigue"), a consequence of a pending refugee crisis from Ukraine.

Second, Russia has consolidated its control over all Russian media covering the conflict in Ukraine. Ukrainian-language broadcast media in the east was effectively neutralized, leaving state-controlled *RT* as the sole source television-based information available to local Ukrainians.[29] Because Russian servers hosted the dominant Russian-language social media platforms—*Vkontakte* and *Odnoklassniki*—the authorities were able to effectively block any pages with a pro-Maidan bent. It also allowed the Russian government to monitor sympathizers of the post-Maidan Ukrainian government, as well as recruit foot soldiers for its pro-separatist proxies. Second, the Kremlin put considerable spin on its portrayal of events in Ukraine, from the 2013-2014 Maidan Revolution, to the takeover of Crimea, to the ongoing war in the East. It portrayed Crimea as being land that historically belonged to Russia. It exaggerated the influence played by Ukrainian nationalists and neo-Nazis among the Maidan protestors, and later those fighting in the Donbas region in order to stoke fear among ethnic Russians and Russian-speaking Ukrainians. By demonizing the enemy, this was tactically important for its proxies, enabling the use of greater violence against their fellow citizens. Finally, the Kremlin-controlled Russian media ignored the presence of Russian soldiers and *spetsnaz* forces in Ukraine, and downplayed the illegality of Russia's land grab of Crimea. Conversely, Russia vastly overstated the role played by the United States in controlling the protests on Maidan and influencing events in the east.

Furthermore, Russian operatives sought to shape the battlefield by directly targeting and manipulating the minds of Ukrainian troops through subversive forms of propaganda and disinformation. In 2017, the Russian authorities created so-called "information operation troops," whose remit, according to Russian Defense Minister Sergei Shoygu, was to spread

"clever and efficient propaganda."[30] The aim of these troops encompasses a mix of strategic communications, psychological operations, and influence activities. They should not be treated as a separate cyberspace-based command, as their means go beyond just conducting cyberwarfare to disrupt networks but also include manipulating the media and planting counterpropaganda in order to control and distort the enemy's cognitive understanding of what is real and what is false. They involve planting fake news stories to stoke irredentist violence. A case in point is the steady stream of disinformation among Russian-language news broadcasts in the south and east of Ukraine threatening locals that Kiev would rescind their right to speak the Russian language. On Kolika Square in 2014, the journalist David Patrikarakos documented how a group of masked men armed with bats and clubs were told that a group of Ukrainian nationalists called *Pravy Sektor* ("Right Sector") was coming "to burn down our tents at 4:00 a.m." Much of the disinformation plays on people's traditional moral values. In 2014, it was also falsely reported by Russian media that Ukrainian soldiers had crucified a small boy.[31] Another popular meme circulated on Russian social media was that of an LGBT (lesbian, gay, bisexual, transgender) activist on the Maidan who harassed a straight passerby to the point of him bludgeoning her to death. The aim of such efforts is to paint the protestors with a broad brush stroke as LGBT activists, a way to sow distrust among rural and more conservative segments of Ukrainian society.[32]

The target of these IW efforts were also the members of the Ukrainian military fighting on the frontline. Shortly after the fighting started in eastern Ukraine in 2014, for example, soldiers deployed to the combat region started receiving "fake texts." The texts were often meant to threaten and demoralize troops in a "grinding" conflict with some texts reading: "Ukrainian soldiers, they'll find your bodies when the snow melts;" "Leave and you will live;" "Nobody needs your kids to become orphans;" "Ukrainian soldier, it's better to retreat alive than to stay here and die;" and "You will not regain Donbas back. Further bloodshed is pointless."[33]

Other texts were aimed to undermine unit cohesion and morale. Texts, often appearing to come from follow soldiers, have claimed the commander had deserted or that Ukrainian forces were being decimated and that "We should run away." Nancy Snow, a professor of public diplomacy at the Kyoto University of Foreign Studies, described this as "pinpoint propaganda." In previous conflicts, leaflets dropped by air or radio messages could easily be ignored—by refusing to pick up and read the leaflet or by tuning to another radio station—but it is nearly impossible to avoid reading text messages sent to one's phone.[34]

Russia combines its IW with kinetic operations, starting with a text message to a soldier, telling him he is "surrounded and abandoned." Ten minutes later, the soldier's family receives (recent contacts) a text message stating, "You son is killed in action." The friends and family likely call the soldier to see if the news is true. Seventeen minutes after the initial text message, the soldier receives another message telling him to "retreat and live" with an artillery strike following shortly thereafter to the location where the large group of targeted cell phones are detected. Thus, in one coordinated action, they use IW to target the soldier and his family and friends and combine it with electronic warfare, cyber electronic warfare, and artillery to produce both kinetic and psychological effects.[35] This is a technique that the Russian operatives are likely to employ in large-scale combat operations as well—blurring the geographical boundaries between the front line and the home front in new and potentially frightening ways.

Likewise, the soldiers of potential allies are not immune to Russian IW. NATO troops deployed in the Baltics and Poland as part of the deterrence mission have also been targeted. Instead of "pinpoint propaganda," soldiers have had their Facebook accounts hacked, data erased, or received messages stating "Someone is trying to access your iPhone" with a map appearing in the text with Moscow at the center of the map. One commander believes the intent of the IW is to intimidate the soldiers and to let them know that Russian intelligence forces are tracking them and their data is at risk.[36]

Russia has also targeted the US military, employing IW in an attempt to decrease its military readiness and that of its NATO allies. Russian media outlets have been known to reach out to the mayors of towns outside of the Hohenfels training area in Germany, asking them if the noise from military training is disruptive to the local population. This is a clear attempt to sow discord between the populations and the US base, with the intent of influencing the German government to put restrictions on military training.[37]

Finally, Russian IW in Ukraine has included attempts of technological interference in political institutions via cyberspace means, with mixed degrees of success. Ukraine provided a laboratory of sorts for Russian hackers who would later interfere more boldly in elections in the United States and in Western Europe.[38] The concept of "weaponized information" was honed in Ukraine to undermine its fledgling institutions and erode public trust. In addition to targeting critical infrastructure—Ukraine's electric grid, government websites, and banks—Russian operatives were active in planting fake news stories. The effectiveness of such operations, however,

are questionable. Examining the effects of Russian propaganda vis-à-vis Russian state-controlled TV in Ukraine, the political scientists Leonid Peisakhin and Arturas Rozenas found the effects to be uneven:

> Ukrainians who were already predisposed in Russia's favor found its media message persuasive. Pro-Russian Ukrainians who watched Russian TV were more likely to vote for pro-Russian candidates in the 2014 presidential and parliamentary elections than were anti-Russian Ukrainians who watched the same programming. Those with anti-Russian views were dissuaded by the Russian media message and became more likely to vote for pro-Western politicians. Individuals with no strong political priors seem not to have been swayed in either direction.[39]

The authors argue that the current erosion of credibility as a result of Russian IW poses not only a threat to Western democracies but also to Russia. Should Russia find itself in a protracted war, not unlike the current proxy conflict it faces in the Donbas, it may face an inflection point where the effectiveness of its propaganda increasingly wanes. This may result in its targeted audiences doubting even the false narratives put out by Russia's bots, hackers, and other spin-masters. Building on previous research, the authors also posit that Russian propaganda does not change minds but rather pushes voters to adapt more extreme points of view and increases political polarization, itself a factor that undermines democracy and liberal norms. Whether this is intended or not, the tactical effect of Russian IW in Ukraine is not to change minds but rather to push people toward the extreme and crowd out the middle. The middle is where democracy thrives, the polar extremes are where it withers and dies.

Conclusion & Countermeasures

The following includes a list of recommended countermeasures the United States and its allies should implement to counteract or deter Russia's use of information warfare.

• *As it did during the Cold War, the United States must contest the IO Battlespace.* The US was heavily invested in IO during the Cold War and the battle of ideas—the idea that capitalism and liberal democracy was superior to communism as an economic and political system—contributed significantly to the victory. But with the end of the Cold War, the United States cashed in its peace dividend and divested itself of national-level institutions, such as the United States Information Agency, that were designed to effectively coordinate and integrate strategic efforts and responses to threats. As a result, the United States has largely ceded the strategic

initiative to peer and near-peer actors by default. The United States must reinvest in strategic institutions, and arm those institutions with the mandate and authorities needed, to enable the United States to regain the initiative in the information environment. As the world's superpower, other nations follow the lead of the United States and if the United States elevated the importance of IO, other nations will follow.

• *Relax Rules of Engagement to Counteract Russian IW with IO.* The United States has done little to actually retaliate against Russia. The 2012 Magnitsky Act demonstrates the effectiveness such measures can have to pressure Moscow and "shame" powerful Russian individuals.[40] Congress has incorporated counter-propaganda funding into its most recent National Defense Authorization Act, in addition to proposed reforms to the Foreign Agent Registration Act and the Committee on Foreign Investment in the United States. However, these acts of legislation do not go far enough. The National Security Council, in its 2017 strategy, calls it "information statecraft."[41] But the United States is limited in its ability to engage in this type of warfare. As one senior NSC staffer put it, "we are not going to have an *RT*. The Russians do. The Iranians do."[42] Still, more innovative, less overt countermeasures are needed to deter, prevent, and punish future Russian aggression in this space, including a more sophisticated and targeted version of Radio Free Europe/Radio Liberty and Voice of America for the Facebook era.

• *Establish credible deterrence against IW.* Deterrence is premised on the threat of inflicting pain on an adversary in order to prevent them from taking an undesirable action. Importantly, the threatened pain must be sufficient to alter the cost-benefit analysis of the target state such that they alter their preferences: a successfully coerced adversary must prefer to avoid pain by complying rather than ignoring the threat and accepting the consequences. Thus, a successful coercive—or deterrent—threat depends on the capabilities to inflict pain and the willingness to do so. It remains to be seen whether the United States has the means to inflict sufficient pain on Russia as retaliation for its IW against our political system. But there should be no doubt as to our willingness to do so. If we are to have any hope of deterring future Russian interference in our democratic processes and institutions, we must make full use of the political and economic tools at our disposal, including sanctions and other forms of financial warfare, to establish a credible threat of pain. Furthermore, it should be clear to all—Moscow especially—that punitive measures are punishment for specific actions against American institutions. This requires shining a bright and very public light on those actions when doing so does not threaten re-

vealing intelligence sources and very publicly declaring the consequences of such actions. Only by regularly and visibly demonstrating to Moscow the cause and effect relationship between IW and punitive measures can we hope to establish a credible deterrent.

• *Provide IO Assistance to Allies.* The United States provides $50 billion in foreign assistance, yet almost none of this goes to support IO efforts.[43] Despite four years of being targeted by Russian IW, Ukraine is on the defensive and seems to have no response to Russian IW efforts. Ukraine should improve its defensive measures to prevent "pinpoint propaganda" and better counter Russia's "fake news." But it cannot do so without significant assistance and outside expertise. While the United States must improve its own capabilities, the United States has the capacity, in terms of expertise and funds, to help Ukraine and other allies.

• *Gather & Analyze More Data on IW*. The United States should catalog all attacks and take an evidence-based approach to identify sources and quantify their effectiveness as a way to track their own progress in deterring attacks and measure variation over time and space. For example, current efforts by the Ukrainian military to broadcast Ukrainian-language radio (Army FM) to the Donbas do not even track the number of listeners, much less the effect such positive messaging has on public attitudes. In the United States, to our knowledge, there is no database yet that tracks this sort of thing.

• *"Protect against Fake News."* Emilio Iasiello, a cyber analyst, recommends "leveraging cutting-edge technology to help identify the fabrications as soon as they emerge. Artificial intelligence and data analytics can be used to detect words or word patterns that might indicate deceitful stories."[44] The United States must do more than simply correct the record. By nature, corrections to the record or fact checks are reactive and are not effective to counter the effects of proactive fake news and Russian propaganda. In the battle of perception, the race to shape the early narrative is often times the decisive fight. Readers rarely care or read corrections, much less disclaimers, especially in an era of social media. To be effective, as Giles recommends, "Countermeasures should focus not on fact-checking but on the deceit—emphasizing that people were conned—and, like the original disinformation, should appeal to readers' emotions rather than their rationality."[45] This is tricky, given that Western governments are supportive of free speech, and so they cannot blanketly restrict news, even if it is false, coming from one country or its citizens.

• *Create a Robust Task Force.* In March 2015, the EU created a StratCom Task Force, whose purpose is to correct disinformation coming from Russian media. This kind of task force should be strengthened, and perhaps be bolstered with the addition of economic sanctions. A similar task force should be created in the United States and properly resourced and given teeth.

• *Establish Stronger Normative Framework for IO much like the Tallinn Manual did for cyberspace.* The trouble with propaganda in the digital age is there are no agreed-upon rules or norms, as there were during the height of the Soviet Union. Also the actors and perpetrators have been decentralized, making attribution more difficult, but also the adherence to norms or rules more problematic. Even though Russia will not abide by covenants agreed to by other states and international bodies, this can at least assist the West to determine the rules for the road for a post-Putin Russia that may determine that IO and the undermining of American influence is not in its best interest.

• *Strengthen retention rates among our allies.* Ukraine is a country teeming with information technology (IT) expertise. Yet, the government and its military have a hard time retaining expertise in this realm, due to higher salaries provided in the private sector. US assistance should be targeted to not only train our partners but be sure they retain their fighters.

• *Strengthen civil society.* Many of the most innovative and effective efforts made to target Russian disinformation and propaganda are coming from civil society groups like InformNapalm, which relies on open-source intelligence and employs volunteer hackers to discredit Russian narratives, or StopFake, which puts out media content to counteract Russian propaganda. These groups have been effective, given recent polls that show that a majority of Ukrainians now say that Russian propaganda constitutes a real threat.

• *Educate service members and their families of Russian IW practices.* American service members and their families must be warned of Russian IW practices and efforts so they are not discovering it for the first time when they are receiving a threatening text message—this will greatly reduce or eliminate the desired effect.

It is worth reassessing the threat of Russian information warfare given the recent doctrinal shift toward large-scale combat operations against peer and near-peer adversaries, which includes a wide spectrum of the use of force. Though it may be tempting to lament the threat that Russian IW poses to American interests and institutions in the 21st century, not to

mention those of our friends and allies, it is important to remember that we have been here before. As noted earlier, the legendary diplomat and scholar George Kennan was entirely familiar with the threat we face today, even if the technologies have changed. But what is important to recognize in his 1948 memorandum on political warfare is not the assessment of such a threat posed by our adversaries. Rather, it is the recognition that the United States must be willing and able to fight political wars just as we were willing to fight conventional wars to secure our interests. Kennan writes:

> Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is 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. They range from such overt actions as political alliances, economic measures (as ERP [the Marshall Plan]), and "white' propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[46]

Kennan's prescription remains just as valid as it did 70 years ago. It is time to recognize the threat that Russian IW poses to America's core interests and respond accordingly.

Notes

1. “Zuckerberg: Facebook is in ‘arms race’ with Russia,” *BBC News*, 11 April 2018, accessed 2 May 2018, http://www.bbc.com/news/world-us-canada-43719784.

2. See Mike Lundy, Rich Creed, “The Return of US Army Field Manual 3-0, Operations,” *Military Review*, November–December 2017.

3. Morgan Chalfant, “Former CIA Director: Don’t call Russian Election Hacking ‘Act of War,’” *The Hill*, 11 April 2018, accessed 20 June 2018, http://thehill.com/policy/cybersecurity/328344-former-cia-director-dont-call-russian-election-hacking-act-of-war.

4. Keir Giles, “Handbook of Russian Information Warfare,” NATO Defense College, November 2016.

5. Edward Lucas and Ben Nimmo, “Information Warfare: What is it and How to Win It?” Center for European Policy Analysis (CEPA) Infowar Paper No. 1, November 2015, 3–4.

6. Andrew Blake, “Michael Hayden, former CIA head, of Russia: ‘We took our eye off the ball,’” *Washington Times*, 1 May 2018.

7. George Kennan, “George F. Kennan on Organizing Political Warfare,” Wilson Center Digital Archive, 30 April 1948, accessed 13 June 2018, https://digitalarchive.wilsoncenter.org/document/114320.pdf.

8. Gabriel Samuels, “NATO puts 300,000 Ground Troops on ‘High Alert’ as Tensions with Russia Mount,” *The Independent*, 7 November 2016.

9. Greg Keeley, “Combatting Russian information warfare—in the Baltics,” *The Hill*, 9 April 2018.

10. Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: 27 November 2012), GL-3.

11. Sophia Porotsky, “Cold War 2.0: Russian Information Warfare,” *Global Security Review*, 8 February 2018, accessed 20 June 2018, https://globalsecuritytyreview.com/cold-war-2-0-russian-information-warfare/.

12. Quoted by Anne Vandermey, “Gaining Followers: The Internet and Cold War-style Propaganda in the Former Soviet Republics, *Wilson Quarterly*, Fall 2016, accessed 20 June 2018, https://wilsonquarterly.com/quarterly/the-lasting-legacy-of-the-cold-war/gaining-followers-the-internet-and-cold-war-style-propaganda-in-the-former-soviet-republic/.

13. Bruce McClintock, “Russian Information Warfare: A Reality that Needs a Response,” RAND Blog, 21 July 2017, accessed 20 June 2018, https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html.

14. Peter Mattis, “Contrasting China’s and Russia’s Influence Operations,” War on the Rocks, 16 January 2018.

15. Maria Snegovaya, “Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare,” *Institute for the Study of War*, September 2015, 10.

16. Vladimir Isachenkov, “Russia announces new branch of military to focus on information warfare amid hacking allegations,” *The Independent*, 22 February 2017.

17. Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly* 60, no. 2, 2016, 189–202.

18. Dustin Volz, "US grand jury indicts 13 Russian nationals in election meddling probe," *Reuters*, 16 February 2018.

19. David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (New York: Basic Books, 2017), 131–151.

20. J.B. Vowell, "Maskirovka: From Russia, With Deception," *RealClearDefense*, 30 October 2016.

21. Snegovaya, "Putin's Information Warfare in Ukraine."

22. Keir Giles, "Countering Russian Information Operations in the Age of Social Media," *Council on Foreign Relations Report*, 21 November 2017.

23. Giles, "Countering Russian Information Operations."

24. Phillip Karber, Joshua Thibeault, "Russia New Generation Warfare," AUSA, 20 May 2016, accessed 14 June 2018, https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare.

25. Lucas, "Information Warfare."

26. McClintock, "Russian Information Warfare."

27. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2, 1978, 167–214.

28. Snegovaya, "Putin's Information Warfare in Ukraine."

29. Michael Kofman, et al., "Lessons from Russia's Operations in Crimea and Eastern Ukraine," *RAND*, 2017.

30. Damien Sharkov, "Russia Announces Information Operations Troops with Counter Propaganda Remit." *Newsweek*, 22 February 2017.

31. Timothy Snyder, *On Tyranny: Twenty Lessons from the Twentieth Century* (New York: Duggan Books, 2017), 97.

32. Patrikarakos, *War in 140 Characters*, 161.

33. Raphael Satter and Dmytro Vlasov, "Ukraine soldiers bombarded by 'pinpoint propaganda' texts," *Associated Press*, 11 May 2017, accessed 14 June 2018, https://apnews.com/9a564a5f64e847d1a50938035ea64b8f Oleksandar Golovko, "Ukrainian Frontline: Cyber + EW + Psyops" PowerPoint brief (Kyiv, Ukraine: General Staff of the Armed Forces, 2018).

34. Satter and Vlasov, "Ukraine soldiers bombarded by 'pinpoint propaganda' texts."

35. Golovko, "Ukrainian Frontline."

36. Thomas Grove, Julia E. Barnes and Drew Hinshaw, "Russia Targets NATO Soldier Smartphones, Western Officials Say," *The Wall Street Journal*, 4 October 2017, accessed 10 May 2018, accessed 14 June 2018, https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402.

37. Interview with military officials in Hohenfels, Germany, on 8 May 2018.

38. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 2017.

39. Leonid Peisakhin, Arturas Rozenas, "When Does Russian Propaganda Work—and When Does it Backfire? Here's What We Found," *Washington Post*, 3 April 2018.

40. The 2012 Magnitsky Act, named after Sergei Magnitsky, a Russian tax accountant who died in prison under mysterious circumstances, punishes Russian officials believed responsible for his death.

41. Peter Grier and Harry Bruinius, "With National Security Strategy, Trump ushers new era of Statecraft," *Christian Science Monitor*, 18 December 2017, accessed 20 June 2018, https://www.csmonitor.com/USA/Politics/2017/1218/With-National-Security-Strategy-Trump-ushers-new-era-of-statecraft.

42. Nadia Schadlow, "Building National Security Strategy," Speech given to Modern War Institute at the US Military Academy at West Point, 2 February 2018, accessed 20 June 2018, https://mwi.usma.edu/event/writing-president-trumps-national-security-strategy-dr-nadia-schadlow/.

43. The US spent $49 billion in 2015; see James McBride, "How Does the US Spend Its Foreign Aid," Council on Foreign Relations, 11 April 2017, accessed 14 June 2018, https://www.cfr.org/backgrounder/how-does-us-spend-its-foreign-aid.

44. Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2, 2017, 62–63.

45. Giles, "Handbook of Russian Information Warfare."

46. George Kennan, "George F. Kennan on Organizing Political Warfare," Wilson Center Digital Archive, 30 April 1948, accessed 10 May 2018, https://digitalarchive.wilsoncenter.org/document/114320.pdf.

Chapter 4
Operation Starkey: The Invasion that Never Was

Colonel Michael R. Taylor, Jr.

Warfare is the art (tao) of deceit.

—Sun-Tzu

In wartime, truth is so precious that she should always be attended by a bodyguard of lies.

—Winston S. Churchill

Operation Starkey was an Allied military deception (MILDEC) conducted in Western Europe during the summer of 1943 that included a false invasion armada targeting the Pas de Calais. This operation was part of a larger deception shaping effort across multiple theaters to gain a position of relative advantage for the invasion of Italy.[1] Starkey failed while Operation Fortitude South, a similar deception conducted in 1944 to set conditions for D-Day's Operation Overlord, succeeded.[2] Why did Starkey fail while Fortitude South succeeded? Can any contemporary lessons be derived for application in future Large-Scale Combat Operations (LSCO)? Was failure linked to limited resources, a flawed plan, Allied internal politics, lack of unity of effort, the vacancy of the Supreme Allied Commander's position, or possibly an entrenched opinion by Adolf Hitler and the German High Command? These possibilities will be explored in search of a plausible theory as to why Operation Starkey failed while looking for insights into future LSCO application.

Military Deception and its Value

Deception, defined by the US military in 1947, is "the art of *causing the enemy* to *derive* and *accept* a particular pre-determined appreciation of friendly dispositions, capabilities, and intentions with the mission of causing him to *react in a pre-selected manner* disadvantageous to the enemy and advantageous to our own forces."[3] More than 70 years later, this definition remains largely unchanged in US Army and Joint Doctrine with the fundamental idea to mislead a military decision maker to take action(s) that gain an advantage for the commander.[4]

Military deception can be described in two variations—ambiguity increasing and, the opposite and more complex, ambiguity decreasing.[5] Ambiguity increasing confuses the military decision maker as to what is truly occurring and can lead to actions such as delaying commitment of

forces or spreading thin to cover multiple dilemmas. The opposite, ambiguity decreasing, focuses the military decision maker on one incorrect threat leading to actions to reinforce or counter, thereby weakening in other areas. Daniel and Herbig noted these two variants of MILDEC are best viewed as a continuum with utter confusion (ambiguity increasing) at one end and convinced misdirection (ambiguity decreasing) at the other—most deceptions blend the two over time.[6]

Widespread use of military deception by nation states was revealed in Sherwin and Whaley's analysis of 93 cases of Western strategic military operations from 1914–1973 which found that 82 percent showed clear evidence that deception was employed—the US and Russia accounting for 41 percent.[7] Their analysis also provided insight into the value of military deception with the probability of achieving victory, given surprise, at 93 percent while without surprise, dropping to 50 percent. The analysis also referenced William R. Harris's monograph that examined an older version of the same data and drew the tentative conclusion that all things being equal, "a country not using deceptive ploys was at a strategic disadvantage against a country that did."[8] Nicholas Rankin aptly reinforces the value by stating: "Deception or deceitfulness in ordinary life is wrong because it corrodes trust, the basic glue of human relationships, but *deceiving your enemy in wartime is common sense*."[9]

Emergence in Allied Operations

The British expanded Allied military deception during World War II from simply achieving surprise over your enemy to a complex art of deceiving the enemy decision maker on a grand scale through calculated manipulation. The British planners persuaded enemy decision makers into taking action, based upon an altered theater-wide or cross-theater reality, enabling the deceiver to gain an advantage for their commander.[10]

Beginning with General Sir Archibald Wavell in the Middle East in 1940 and encouraged by Prime Minister Winston Churchill, the British built their military deception capability from the tactical to the strategic level out of necessity to counter German strength and compensate for weakness.[11] The flair for deception possessed by both leaders dated back to World War I but with widely differing experiences. General Wavell's motivation for deception found its genesis at the tactical level during the 1915 Ypres attack where he was wounded while losing two-thirds of his brigade due to continuous German artillery fire—impressing the need for new ways of waging war including deception to avoid mass slaughter.[12] Winston Churchill's roots as a deception proponent was established in

1914 at the strategic level as the First Lord of the Admiralty where he directed creation of a dummy fleet to mislead the Germans.[13] Daniel and Herbig aptly described the British motivation for expanding deception during World War II: "When outcomes are critical, adversaries are encouraged to make use of every capability, every advantage, to insure victory or stave off defeat."[14]

Leading up to 1943, the British successfully employed deception in the Middle East and most recently in coordination with the US during Operation Torch in North Africa. The US and British recognized the need for continuous deception operations across multiple theaters and agreed to geographically split responsibilities. The US would be responsible for the Pacific theater led by the Joint Security Control (JSC) and the British for the Mediterranean and European theaters led by the London Controlling Section (LCS)—both organizations would collaborate and synchronize deception efforts going forward. The Allies would now focus their deception efforts in 1943 on Western Europe to gain a position of relative advantage over the Germans in the subsequent battles for southern and eastern Europe.[15]

The Strategic Situation and Creation of COSSAC

January 1943 opened with the Allied offensive in North Africa continuing, the Russians battling the *Wehrmacht* on a colossal scale on the Eastern Front, and the British and American forces slowly massing in England preparing for a future cross-Channel invasion.[16] In January, President Franklin Delano Roosevelt, Prime Minister Churchill, and the Combined Chiefs of Staff attended the Casablanca Conference where they designated the invasion of Sicily as the year's priority.[17] Allied leadership discussed the importance of minimizing the ability of the Germans to reinforce in Italy and Russia, as well as a future cross-Channel invasion. The conference ended with the summary that: "plans should be produced for a return to the Continent in the event of German weakening or collapse and *for deceptive operations to be conducted during 1943* . . . and it was recognized that the full-scale, cross-channel attack could not take place before 1944."[18]

The Casablanca Conference required a new headquarters to plan for a return to the European continent and for deception operations in support of that objective. Major General Sir Frederick E. Morgan was designated as the Chief of Staff to lead this new headquarters, pending the appointment of a Supreme Commander in 1944.[19] The deception guidance issued at Casablanca later transformed into Operation Starkey, planned and con-

ducted by the new headquarters titled Chief of Staff, Supreme Allied Commander (COSSAC).

COSSAC formed in April 1943 as a planning staff with the intent to transform into an operational command once a Supreme Commander was designated. Major General Morgan led COSSAC as the Chief of Staff but did not possess command authority over component commanders, each of whom were charged with specific missions.[20] Major General Morgan recognized this weakness and pursued gaining command authority, through the British Chiefs of Staff, to transform COSSAC's orders from recommendations into actual directives and effectively arbitrate disagreements on implementation.[21]

As COSSAC formed, Major General Morgan created OPS B, a secretive staff section led by Lieutenant Colonel John J. Read, to plan and carry out deception planning and operations.[22] OPS B collaborated with the intelligence community and the LCS, led by Colonel John Bevan, which supported and coordinated the Allied deception efforts across the European and Mediterranean theaters to mislead the German High Command, *Oberkommando der Wehrmacht* (OKW), and ultimately Germany's primary military decision maker, Adolf Hitler.[23] The LCS passed disinformation through a British controlled network of double-agents in England also called "special means," which was guided by feedback from OKW's communications broken by the Ultra signals intelligence (SIGINT). This close coordination between deception planning, operations, and the intelligence community would pay dividends during deception operations in 1943–44.[24]

Starkey on Paper

Military deception plans in World War II consisted of three basic components: a mission statement, the deception story, and the means of implementation. The mission statement described what the commander wanted the enemy decision maker and target to do, the deception story detailed what the deception planners wanted the enemy to think was reality, and the means of implementation (physical, signals, double agents, etc.) were what the enemy would see to make the story plausible, and ultimately lead to the deception target taking an action (or series of actions) disadvantageous to the enemy and advantageous to the commander. Operation Starkey included all three components.[25]

Cockade was an umbrella plan, with Operation Starkey as the main effort of three deception operations in 1943.[26] This plan was intended to accomplish the Chiefs of Staff directive to plan for: "an elaborate cam-

ouflage and deception scheme extending over the whole summer with a view to *pinning the enemy in the West* and keeping alive the expectation of large-scale cross Channel operations in 1943. This would include at least one amphibious feint with the object of *bringing on an air battle* employing the Metropolitan Royal Air Force and the US 8th Air Force."[27] Central to the entire plan was persuading Hitler, the military decision maker and deception target, and the OKW, who filtered his intelligence, that the Allies would conduct a cross-Channel operation in the summer of 1943. Plan Cockade would create a story consisting of both real and fictitious means of implementation leading Hitler to choose to keep forces in Western Europe as a hedge against this threat while committing the German Air Force (or *Luftwaffe*) to battle—shaping at the strategic level across multiple theaters to relieve pressure off the Russians while creating a position of relative advantage for the invasion of Sicily and Italy.

The first of Plan Cockade's three operations was Starkey, consisting of an actual "amphibious feint to force the *Luftwaffe* to engage in intensive fighting over a period of about 14 days, by building up a threat of an imminent large-scale British landing in the Pas de Calais area" culminating between 8 and 14 September.[28] The second operation, Wadham, persuaded the Germans that a large-scale American invasion of Brittany from both England and the US would follow Starkey in late September.[29] This operation, per the deception story, would later be postponed until November and then cancelled, to better emphasize Starkey to the OKW. The final operation, Tindall, would fix German forces in Norway by threating an invasion of Stavanger in mid to late September.[30] This operation would also be cancelled to support the deception story of an Allied focus on supporting Starkey and Wadham. Each operation employed fictitious divisions—Starkey commanded 14 British and Canadian, Wadham five US, and Tindall five Scottish.[31] Starkey was the only operation that employed actual forces and key to the success of the overall Allied deception plan in 1943.

Operation Starkey was commanded by Air Marshal Sir Trafford Leigh-Mallory, Commander-in-Chief, Fighter Command in coordination with Major General Ira C. Eaker, Commanding General, US 8th Air Force along with the Naval and Army commanders designated by the Commander-in-Chief Portsmouth and the Commander-in-Chief Home Forces, respectively.[32] Tindall and Wadham were commanded by a combination of Army, Navy, and Air Force leaders with COSSAC having overall responsibility for Cockade, as the coordinating headquarters.[33]

The COSSAC planners chose the Pas de Calais as the target for Starkey's amphibious attack—providing the "greatest advantage" to Allied

fighters to engage the *Luftwaffe*.[34] The Pas de Calais was considered "the most heavily fortified . . . sector of the whole coast of France" and COSSAC determined that "no assault against it could be attempted without considerable prior bombardment both from the air and from the sea."[35] The air and sea bombardment was deemed by COSSAC planners as critical observable means that would provide indications to OKW of an impending attack. COSSAC planned to gradually conduct air, land, and sea observable means consistent with amphibious preparations to persuade OKW that the Allies would invade, forcing commitment of the *Luftwaffe* to battle.

The Starkey air plan massed 45 British and 15 American fighter squadrons opposite the Pas de Calais supporting the invasion and *Luftwaffe* battle.[36] The plan also gradually diverted air activity, including bombing and reconnaissance, to the Pas de Calais and secondary to Brittany beginning on 15 June.[37] Fourteen days prior to the fictitious invasion, the plan diverted 3,000 US day heavy bombing missions and the same number of British night heavy bombing missions to targets that created the pattern of an impending invasion as the first critical observable. The heavy bombing missions were determined by the COSSAC planners to be: "the minimum amount of aerial activity needed to convince the enemy that a genuine invasion was in prospect."[38] This is an example of deceptive fires being employed as observable means to reinforce the deception story.

The naval plan assembled landing craft in the Channel by 1 September and interrupted the coastal convoy program fourteen days prior to the invasion to: "simulate a concentration of shipping in ports prior to the launching of a large-scale attack."[39] The planners determined that massing 450 landing craft would serve as a second critical observable means to convince the Germans that the invasion was more than just another small Dieppe raid, conducted by the Canadians against France in August 1942.[40] The shipping concentration in ports would consist of no less than 130 ships to simulate a break in the convoys.[41]

Additional naval actions included British Commando raids portraying coastal reconnaissance and massing "essential naval escorts and minesweeping flotillas along with two 'R' Class battleships for bombardment of long-range German coast artillery in coordination with air attacks."[42] COSSAC indicated that the presence of the two battleships would act as "cheese in the mousetrap" to draw the *Luftwaffe* into battle and serve as a third critical observable for the deception plan.[43] The naval invasion forces would consist of two battleships, 12 destroyers, 29 minesweepers, 59 other ships, and various landing craft.[44]

Starkey's land forces consisted of fourteen fictitious British and Canadian divisions—the fourth and final critical observable means that would indicate a future attack.[45] Actual land forces committed amounted to less than two divisions including the Royal Marine Division, five commandos, a parachute brigade, an air-landing brigade, and various smaller Canadian units.[46] COSSAC determined that the available land forces in England would not be capable of convincing the Germans of an impending invasion, so they devised a plan to mislead the OKW into increasing their assessment of the Allied Order of Battle.[47] The LCS began preparing for this requirement in January by feeding disinformation to the Germans through double-agents such as GARBO, a collection of German spies that had been turned—either coercively or willingly—by British Military Intelligence.[48] COSSAC would create two fictitious Army Corps—the VIII and the XII—consisting of 60,000 non-existent men through observable means such as false camps and dummy vehicles, unit markings, signals traffic that replicated units, and the LCS efforts.[49] To protect operations security (OPSEC) the British government would enact strict security measures in southeastern England beginning on 1 August for six weeks to portray heightened readiness in preparation for an invasion.[50]

Foreshadowing Starkey's Demise

Deception planning began in January with the LCS and transitioned to OPS B in April—a critical month for the future of Starkey.[51] On 14 April, General Morgan met with Major General's Sir Leslie Hollis, Secretary to the Chiefs of Staff Committee, and Sir Hastings Ismay, Military Deputy Secretary to the War Cabinet, to discuss preventing command level conflicts due to competing priorities of invasion training, the Combined Bomber Offensive against Germany, and Allied deception operations—exacerbated by the lack of a Supreme Commander.[52] The meeting minutes recorded:

> Deception plans would be drawn up by COSSAC, but they would have to be implemented by senior Service commanders who might be reluctant to give them priority over operational or training requirements. In order to convince those commanders of the importance of deception he [Hollis] suggested that the situation should be explained to them at a Chiefs of Staff Conference, perhaps with the Prime Minister in the Chair.[53]

On 17 April, Major General Morgan addressed his staff at the first meeting of COSSAC with: "In spite of the fact that it is quite clear that neither I nor you have by definition any executive authority, my idea is that

we shall regard ourselves in the first instance as primarily a coordinating body."[54] Major General Hollis published a letter on 22 April to the Chiefs of Staff stating: "It is the second phase, namely, the execution of the deception which is complicated. The executive orders for troops to march and for troops and aircraft or Air Force personnel to move for deception purposes, must come from the Naval, Army, and Air Commanders-in-Chiefs concerned."[55] Later in the same letter, Hollis echoed his 14 April minutes by proposing a meeting of all Commanders-in-Chiefs, possibly under the chairmanship of the Prime Minister, to explain that effective deception may interfere with training and movement of forces.[56]

The Chiefs of Staff responded on 27 April and, for unknown reasons, declined to support a combined Prime Minister and Commanders' conference; instead ordered COSSAC to request the commanders cooperate in the preparation and invite them "to take the necessary executive action" which would preserve the current chain-of-command.[57] This Allied decision would begin the demise of Operation Starkey.

On 19 May, Hitler, the deception target, held a Situation Conference with his generals, a week after the last Axis forces surrendered in North Africa, and stated that: "Nothing is going to happen in the west; I'm fully convinced of that. If they want to attack somewhere, then they'll only attack in Italy, and in the Balkans, naturally."[58] This opinion was a stark change from the past two years focused on Western Europe invasion fears and would color future German reporting and analysis of Starkey preparations and ultimately Hitler's reaction, or lack thereof—all but sealing the fate of the Allied operation.

The Execution of Operation Starkey

The implementation of Starkey began in May with LCS double-agents passing calculated disinformation reports as observable means to the Germans consisting of invasion preparation rumors, large-scale cross-Channel bomber attacks, observations of offensive troop concentrations, and government announcements supporting the three deception operations under Plan Cockade.[59] Also in May, COSSAC determined that the lack of landing craft was not "sufficient to give an air of realism to the invasion preparations" causing alarm and discussions of abandoning the amphibious feint, but in the end compensated by the employment of 175 dummy landing-craft.[60]

On 3 June, Operation Starkey was issued as part of Plan Cockade to the Chiefs of Staff.[61] The date of the invasion was set between the 8th and

the 14th of September and timed with Operation Avalanche, the invasion of Italy.[62]

On 7 June, Major General Eaker, Commanding General, US 8th Air Force sent a memo to Lieutenant General Jacob L. Devers, Commander European Theater of Operations, US Army (ETOUSA) arguing against supporting Starkey.[63] Major General Eaker wrote that: "the Combined Chiefs of Staff have given this Air Force a Directive against industrial targets" and the diversion of 3,000 heavy bomber missions for 14 days would force abandonment of the Combined Bomber Offensive.[64]

On 10 June, Brigadier General R. W. Barker, the ETOUSA G-5, wrote to Lieutenant General Devers outlining the US commitments to Cockade and impact on the Combined Bomber Offensive.[65] He wrote that: "It should be determined which of these two operations take priority, realizing that if it is Cockade, the Combined Bomber effort is practically suspended for a period of 14 days, and at the same time realizing if it is not suspended, Operation Cockade will probably fail to accomplish its objective."[66]

Major General Eaker would get his way and the Combined Bomber Offensive remained the priority. The US 8th Air Force would support Starkey with only training units and missions diverted due to weather highlighting the need for COSSAC command authority or a supreme commander to determine priorities.[67] On 15 June the Allies began shifting bombing and air reconnaissance to the Pas de Calais and Brittany.[68]

Also in June, First Sea Lord Admiral Sir Dudley Pound objected to the use of the two "R" class battleships and argued that they "should not be endangered in a fake operation" and could not reduce coastal artillery.[69] He invoked past memories of the loss of two capital ships to Japanese air attack in December 1941 to reinforce the point that if sunk, the German victory could impact British morale. Vice-Admiral Lord Louis Mountbatten, Chief of Combined Operations argued that battleships were essential, and Major General Morgan claimed that the *Luftwaffe* would not take the bait unless included in the invasion force.[70] The battleships were ultimately removed.

On 11 July, the OKW informed Field Marshal Gerd von Rundstedt, Commander-in-Chief West (OB West), the Allied focal point on mainland Europe was in the Mediterranean.[71] Nine days later, von Rundstedt reported that the removal of German formations from Western Europe provide incentive for an Allied invasion; the Allies have sufficient air and naval forces to invade.[72]

British Commandos planned 14 raids on the French Channel coast for July and August called Operation Forfar.[73] Only eight were conducted, and none were detected by the Germans resulting in no discernable counteractions from German decision makers. In mid-August the British instituted OPSEC measures in southern England to portray heightened readiness levels.[74] The Allies also conducted supply drops to French resistance forces and carefully provided instruction via British Broadcasting Corporation (BBC) radio to only take action when specifically instructed by London, sparing loss of credibility and lives key to the actual invasion in 1944.[75]

On 9 August, COSSAC reported that Starkey was gathering momentum, and by mid-August that the enemy displayed signs of beginning to react to reconnaissance and bombing activities.[76] On 23 August COSSAC assessed that German preliminary reactions to Starkey were as great as could be expected.[77]

On 24 August, the Commander-in-Chief, Bomber Command, Air Chief Marshal Sir Arthur Harris received the Starkey bombing plan from the Air Ministry and replied angrily over "receiving peremptory orders" diverting British bombers and that Fighter Command (overall responsible for Starkey) assumes "the right to call on Bomber Command aircraft at will"—highlighting the personality conflict between fighter and bomber community leadership and the need for a supreme commander to arbitrate and determine priorities.[78] The Vice Chief of the Air Staff pointed out that Starkey would interfere with the Combined Bomber Offensive which was the highest priority.[79] Bomber Command would support Starkey with only training units and Wellington squadrons, and surge up to 200 sorties on the final night of the operation.[80]

False Invasion

On 25 August, Allied bombing began to increase in the Pas de Calais and Brittany areas—nearly doubling leading up to 8 September but almost half of the missions were cancelled due to weather which would continue to cause challenges.[81] Also, on 25 August COSSAC cancelled Tindall preparations per the deception story to focus OKW's attention on Starkey.

Allied landing craft began to mass in points along the Channel in preparation for the invasion convoy. Weather also disrupted minesweeping operations—only three flotillas cleared the passage across the channel and received a small amount of gunfire.[82] Major General Morgan reported on 2 September to the Chiefs of Staff that weather has disrupted plans for air and minesweeping operations and given the limited German reaction,

recommended cancelling the invasion convoy.[83] The Chiefs of Staff did not agree and instructed Starkey to continue as planned.

In early September, von Rundstedt's staff questioned the observed invasion preparations and whether they are intended to: "entice German reserves there and to pin them down."[84] On 5 September, the LCS agent GARBO passed through his network to the Germans that the invasion will begin on 8 September.[85] A day later von Rundstedt admitted that: "it could not be laid down with certainty" that a major attack across the Channel was imminent; he noted that all necessary measures have been taken to meet it.[86] On 8 September, GARBO reported that Allied troops were conducting final preparations and landing craft were massing.[87] The final preparations and loading were part of Operation Harlequin, an actual major exercise involving British and Canadian divisions embarking onto transports to support the deception operation; units disembarked before the invasion convoy sailed.[88]

The morning of 9 September, the invasion began with a convoy of 30 vessels sailing to within 10 miles of the French coast, and then returning under a smoke screen.[89] A second convoy of landing craft sailed eastward, replicating a landing force, and then returned three hours later. The German defenses on the Pas de Calais were fully alerted but the movement of the invasion fleet was not reported as significant. Operation Avalanche, the invasion of Salerno, Italy commenced on 9 September, and most likely diverted the attention of OKW.[90] Following the return of the convoys, the Chiefs of Staff issued a general statement to the British media regarding the invasion preparations and Starkey, describing the event as only an exercise.[91] GARBO reported to the OKW that troops have disembarked and "it appears that the operation has been suspended."[92]

Post-operation Analysis

With the completion of Starkey, Air Marshal Sir Trafford Leigh-Mallory, who commanded the operation, reported that the air and naval actions did not produce a physical reaction by the Germans; only the minesweeping provoked a response.[93] He further noted the desired air battle with the *Luftwaffe* never materialized. COSSAC Intelligence reported there was no evidence of any military defensive moves in France:

> On the contrary, the movement of troops from France to Italy had not been interrupted, and the *German forces had not therefore been pinned down away from the active fronts*. Apparently the enemy had realized that the Allies were in no position to undertake

extensive operations in northwest Europe at the same time as they were engaged so fully in the south. [emphasis added][94]

German divisions in Western Europe were steadily reduced from 45 in May to 35 in September.[95] Operation Starkey did not achieve the desired actions by Hitler and the OKW to keep forces in Western Europe while drawing the *Luftwaffe* into battle—what contributed to this failure?

A plausible theory for Operation Starkey's failure can be attributed to two overarching factors—lack of COSSAC's command authority combined with a vacant Supreme Allied Commander's position and, more importantly, an entrenched opinion by Adolf Hitler and OKW. Both of these factors created cascading second and third order effects that would further diminish chances of deception success.

First, Major General Morgan's lack of command authority as COSSAC and the larger issue of the vacant Supreme Commander's position opened the door for internal Allied politics, personality, and prioritization conflicts amongst the various commanders supporting the deception. COSSAC was designated only as a planning and coordinating headquarters responsible for Cockade while execution of each deception operation was delegated to a Commander-in-Chief, but with only the authority to ask and coordinate with peers; not to task and enforce support. Major General Morgan acknowledged the Supreme Commander would not be designated until late 1943 and recognized the challenges resulting from his lack of command authority early in the planning process. He attempted to address the issue through the Chiefs of Staff by asking for a meeting with all of the commanders, potentially chaired by the Prime Minister, to convey the importance of supporting the deception operation. Major General Morgan was rebuffed by the Chiefs of Staff and informed that COSSAC should "invite them to take action" and the commanders must provide the orders.[96] The lack of an empowered COSSAC led to independent component commander decisions which on their own were correct but in aggregate would be detrimental to a unified Allied deception effort.

Command of Operation Starkey was, in name only, given to the Commander-in-Chief Fighter Command and coordinated with Commanding General US 8th Air Force and the Naval and Army Commanders-in-Chief respectively—all equals with none given authority to resolve disagreements or determine priorities and each charged with independent missions. This created friction and prioritization conflicts between commanders on whether to support Operation Starkey, the Combined Bomber Offensive, individual training efforts, or to protect key naval forces for future op-

erations. For example, Major General Eaker, US Commanding General, 8th Air Force identified the conflict between supporting Starkey and the Combined Bomber Offensive and chose to appeal to Lieutenant General Devers, senior US commander, instead of through Fighter Command and COSSAC to resolve—US bombers would remain focused on the combined offensive knowing the decision would doom Starkey. Similar conflicts emerged with the British bombers and battleship support. Each of these conflicts were addressed by the individual commanders, leaving COSSAC's Plan Cockade and the main effort, Operation Starkey, a hollow plan—reducing critical observable means such as US and British bombing missions required to build a plausible deception story.

A COSSAC empowered with command authority or designation of a Supreme Commander would have established unity of command and led to priority of support decisions for the components to implement—ultimately holding commanders accountable for resourcing the deception operation while ensuring Allied unity of effort. This point was evidenced in the later Fortitude deception plan issued on 26 February 1944 stating that the Allied air, naval and land force commanders "will be responsible to the Supreme Commander for . . . they will also be responsible for making preparations . . . [and] they will adhere to the broad design of Plan Fortitude."[97] This document was clearly directive in nature and backed by the authority of the Supreme Commander—the antithesis of COSSAC's Plan Cockade and Operation Starkey. Even with an empowered COSSAC ensuring implementation of critical observables required to build a plausible story there is no guarantee that Starkey would have achieved its desired effects—especially if Hitler, the deception target, discounted intelligence reporting that did not agree with his opinion of future Allied actions.

The second overarching factor contributing to Starkey's failure was, unbeknownst to COSSAC, Adolf Hitler and the OKW had changed their opinion in May that an invasion of Western Europe would not occur in 1943. This predisposition was formed after losing North Africa, and now faced with predicting the location of the next Allied attack either in Italy, the Balkans, or Western Europe—Hitler chose Italy and the Balkans.

Given that Operation Starkey was fundamentally an ambiguity-decreasing deception, the Allies' lack of knowledge of Hitler's opinion and predisposition in May 1943 proved fatal. The lack of understanding of the deception target's bias, tendencies, and predispositions ultimately led to an operation that was doomed from the start. Daniel and Herbig highlight that deceivers would have a higher chance of success going with the grain or predisposition of the decision maker than against—altering predisposi-

tions are the exception not the norm. Operation Starkey would most likely have failed even with a fully supported series of critical observable means including: an enlarged Order of Battle sufficient to conduct an attack, creating a bombing pattern matching an impending invasion which was an indicator tracked by OKW in 1944, employing expected naval battleship bombardment support, and massing enough landing craft to enable an amphibious assault in force.[98]

One additional factor for consideration was the impact of weather both in terms of the diversion of Allied effort, and the simultaneous impact it had on Germany's ability to detect and report on observables. Over half of the limited bombing missions conducted in the Pas de Calais and Brittany areas over 14 days leading up to the "invasion" were cancelled due to weather. Minesweeping operations across the channel were also limited in sorties due to weather—resulting in minimal detection and reporting from the Germans. Weather negatively impacted implementation of these few observables, reduced ability of the Germans to detect and report, and likely added to the growing challenge to success.

Given the overall failure, Operation Starkey was successful in setting conditions for the 1944 deception—Operation Fortitude South under Plan Bodyguard. The COSSAC history notes that Starkey was: "useful as a rehearsal to improve coordination and support by air, naval, army, and civil authorities in advance of Overlord."[99] The means and methods used by OPS B and LCS in coordination with the intelligence community and Ultra were tested for 1944. This included building up the double agent GARBO network's credibility with OKW and establishing a proven channel to Hitler for deception which would be exploited over the coming years.[100] Also the fictitious Allied Order of Battle was increased to 43 divisions in October, according to the OKW assessment, even though the actual strength was only 17 divisions.[101] In addition to a rehearsal, on 7 September Major General Morgan received executive authority from the Chiefs of Staff, too late for Operation Starkey, but would allow COSSAC to become directive with the Fortitude deception planning and implementation; continuing with General Eisenhower after his arrival in January 1944. These individual successes would ultimately combine and pay dividends during the "shaping" Operation Fortitude that would set conditions for the "decisive" Operation Overlord and the Allies return to continental Europe in 1944.

Contemporary Lessons for Large-Scale Combat Operations

The 1943 Operation Starkey provides four useful military deception lessons for contemporary leaders to consider in planning and conducting future Large-Scale Combat Operations. These insights are: employing MILDEC increases chances of victory during LSCO; the commander is key to effectively incorporating into plans and operations; importance of staff and intelligence community collaboration in understanding the decision maker's predispositions to build a plausible deception; and the need for Services to invest and train in the employment of MILDEC observables to reinforce future deceptions.

First, employing MILDEC increases chances of victory during Large-Scale Combat Operations. Historically a nation that does not employ deception will be at a disadvantage against those that do. We can anticipate our future adversaries will employ deception given historical widespread use to counter our strength and compensate for weakness. US forces, barring unforeseen overmatch, will need to employ MILDEC to do the same to gain a position of relative advantage against a future peer and win during Large-Scale Combat Operations—it is common sense in warfare.

Second, the commander has a key role in identifying, in the early stages of planning, what he wants the adversary military decision maker to do that provides a position of relative advantage for decisive operations—the commander's deception mission statement. This statement drives incorporation of deception into the organization's planning and operations and focuses subordinate commander's and staff efforts to prioritize and support. A commander's emphasis is key to staff and intelligence collaboration, resource allocation, and overall deception success—gaining a critical advantage against a future peer adversary during LSCO.

Third, the staff and intelligence community must collaborate to identify the military decision maker's predispositions and then determine how best to achieve the commander's deception mission. As evidenced with Starkey, the deception target's opinions, biases, and predispositions are critical and must be illuminated to build a plausible deception story for implementation. The deception staff's collaboration with the intelligence staff and community begin with gaining shared understanding during initial planning and continues through execution, ensuring feedback and adjustment to the story over time via observable means, and leading to accomplishing the deception mission.

Finally, there is a need for Services to invest and train in the employment of MILDEC observables to reinforce deception given utility in LSCO. The Allies created staffs and organizations to conduct deception operations and create observables such as false camps, dummy vehicles, ships, and planes, and signals traffic replicating fictitious units. These observables supported deception operations at the tactical level and applied to larger strategic efforts like Starkey. In the contemporary environment there is utility in creating observables—physical and virtual—to deceive adversary collection efforts and support deception. Services should explore utility of creating observables that can be employed from tactical to strategic level to deceive future adversaries including their intelligence collection capabilities and then integrate into training to ensure effective application in future Large-Scale Combat Operations.

As we look to future LSCO, our motivation for employing deception should mirror that of the British in 1943: "When outcomes are critical, adversaries are encouraged to make use of every capability, every advantage, to insure victory or stave off defeat."[102] Operation Starkey should be recognized not for its failure but instead for its service as a training opportunity allowing the deceivers to hone their skills and identify lessons learned. Operation Starkey failed to achieve its objectives but served as a stepping stone for the successful Fortitude South deception in 1944 and, more than 70 years later, insights on how to leverage MILDEC to win against a peer during large-scale combat operations.

Notes

1. Michael Howard, *Strategic Deception in the Second World War* (New York: Cambridge University Press, 1990), 75.

2. Roger Hesketh, *Fortitude: The D-Day Deception Campaign* (New York: Overlook Press, 2000), 379.

3. US National War College, *Presentation on Measures to Deceive the Enemy* (Bolling Air Force Base: Air Force Historical Studies Office, 1947), 5; emphasis added.

4. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: 2017), 2-28.

5. Department of the Army, Field Manual (FM) 6-0 Change 1, *Commander and Staff Organization and Operations*, (Washington, DC: 2015), 11-3.

6. Donald C. Daniel and Katherine L. Herbig, *Strategic Military Deception* (New York: Pergamon Press, 1982), 7.

7. Daniel and Herbig, 185.

8. Daniel and Herbig, 185.

9. Nicholas Rankin, *Churchill's Wizards: The British Genius for Deception, 1914–1945*, (London: Faber and Faber, 2008), 420; emphasis added.

10. Howard, *Strategic Deception in the Second World War*, ix.

11. US National War College, *Presentation on measures to deceive the enemy*, 1.

12. Nicholas Rankin, *Churchill's Wizards*, 50.

13. Rankin, xiii.

14. Daniel and Herbig, *Strategic Military Deception*, 12.

15. Howard, *Strategic Deception in the Second World War*, 71.

16. Howard, 61.

17. Nicholas Rankin, *Churchill's Wizards*, 373.

18. Historical Subsection, Office of Secretary, General Staff, Supreme Headquarters, Allied Expeditionary Force, *History of COSSAC*, (Bolling Air Force Base: Air Force Historical Studies Office, 1944), 1; emphasis added.

19. Historical Subsection, *History of COSSAC*, 1.

20. Historical Subsection, *History of COSSAC*, 6.

21. Howard, *Strategic Deception in the Second World War*, 74.

22. Hesketh, *Fortitude*, ix.

23. Howard, *Strategic Deception in the Second World War*, 72.

24. Hesketh, *Fortitude*, ix.

25. US National War College, *Presentation on measures to deceive the enemy*, 5.

26. Howard, *Strategic Deception in the Second World War*, 75.

27. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, (Bolling Air Force Base: Air Force Historical Studies Office, 1943) 1; emphasis added.

28. Howard, *Strategic Deception in the Second World War*, 75.

29. Howard, 75.

30. Howard, 75.

31. Howard, 75.
32. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 2.
33. Chief of Staff, Supreme Allied Commander, 2.
34. Chief of Staff, Supreme Allied Commander, 6.
35. Chief of Staff, Supreme Allied Commander, 2.
36. Charles Cruickshank, *Deception in World War II* (Oxford: Oxford University Press, 1979) 62.
37. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 3.
38. Cruickshank, *Deception in World War II*, 62.
39. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 3.
40. Cruickshank, *Deception in World War II*, 68.
41. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 3.
42. Chief of Staff, Supreme Allied Commander, 3.
43. Historical Subsection, *History of COSSAC*, 18.
44. Cruickshank, *Deception in World War II*, 62.
45. Howard, *Strategic Deception in the Second World War*, 75.
46. Cruickshank, *Deception in World War II*, 62.
47. Howard, *Strategic Deception in the Second World War*, 75.
48. Howard, 75.
49. Cruickshank, *Deception in World War II*, 62.
50. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 3.
51. Hesketh, *Fortitude*, xvi.
52. Howard, *Strategic Deception in the Second World War*, 74.
53. Howard, 74.
54. Historical Subsection, *History of COSSAC*, 2.
55. Howard, *Strategic Deception in the Second World War*, 74.
56. Howard, 74.
57. Howard, 74.
58. David Kahn, *Hitler's Spies: German Military Intelligence in World War II* (New York: MacMillan Publishing Company, 1978), 480.
59. Howard, *Strategic Deception in the Second World War, 77*.
60. Historical Subsection, *History of COSSAC*, 19.
61. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 1.
62. Chief of Staff, Supreme Allied Commander, 1.
63. "Ira C. Eaker Letter to Lt Gen Jacob L. Devers, CG ETOUSA concerning Cockade," Air Force Historical Studies Office, 1943, 1.
64. "Ira C. Eaker Letter to Lt Gen Jacob L. Devers," 1.
65. R.W. Barker, *US Commitments to Operation Cockade* (Bolling Air Force Base: Air Force Historical Studies Office, 1943) 1.
66. Barker, *US Commitments to Operation Cockade*, 2.
67. Cruickshank, *Deception in World War II*, 63.
68. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 3.
69. Cruickshank, *Deception in World War II*, 62.
70. Cruickshank, 62.
71. Howard, *Strategic Deception in the Second World War*, 79.

72. Howard, 79.
73. Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (New York: Scribner, 2004) 486.
74. Chief of Staff, Supreme Allied Commander, *Plan Cockade*, 3.
75. Holt, *The Deceivers*, 97.
76. Historical Subsection, *History of COSSAC*, 19.
77. Historical Subsection, 19.
78. Cruickshank, *Deception in World War II*, 63.
79. Historical Subsection, *History of COSSAC*, 18.
80. Historical Subsection, 18.
81. Historical Subsection, 19.
82. Historical Subsection, 19.
83. Historical Subsection, 19.
84. Howard, *Strategic Deception in the Second World War*, 80.
85. Howard, 78.
86. Historical Subsection, *History of COSSAC*, 19.
87. Historical Subsection, 78.
88. Cruickshank, *Deception in World War II*, 67.
89. Howard, *Strategic Deception in the Second World War*, 79.
90. Cruickshank, *Deception in World War II*, 72.
91. Historical Subsection, History of COSSAC, 20.
92. Howard, *Strategic Deception in the Second World War*, 78.
93. Historical Subsection, *History of COSSAC*, 21.
94. Historical Subsection, 21.
95. Howard, *Strategic Deception in the Second World War*, 79.
96. Howard, 74.
97. Hesketh, *Fortitude*, 379.
98. Kahn, *Hitler's Spies*, 498.
99. Historical Subsection, *History of COSSAC*, 21.
100. Public Record Office, *Garbo: The Spy Who Saved D-Day*, (Public Record Office Publications, 2000) 146.
101. Howard, *Strategic Deception in the Second World War*, 76.
102. Daniel and Herbig, *Strategic Military Deception*, 12.

Chapter 5

The 1948 War For Palestine: "What Kind of War Was This?"

Sergeant First Class Brandon S. Riley, Michael E. Kitchens,
and Colonel Matthew J. Yandura

> *In our democracy, where the government is truly an agent of the popular will, military policy is dependent on public opinion, and an organization for war will be good or bad as the public is well informed or badly informed regarding the factors that bear on the subject.*[1]
>
> —General George C. Marshall,
> 1939 Address to the Washington Historical Society

> *At its heart . . . the conflict has remained the same: a struggle between the original Palestinian majority of Arabs to retain their status and land against waves of immigrant Jews laying a claim to their biblical heritage.*[2]
>
> —Donald Neff, Author of Fallen Pillars

The question of Palestine, the tiny, seemingly insignificant slice of land the size of New Jersey that borders three continents, has confounded experts of international affairs for a 120-plus years and involved no less than 21 consecutive US presidents. The 1948 War for Palestine occurred on the heels of World War II—the former claiming approximately 19,900 lives (approximately 13,500 Arab and 6,400 Israeli). The "1948" War for Palestine actually began on 29 November 1947, with United Nations (UN) Resolution 181, an act that partitioned Palestine in two. The war ended on 20 July 1949, with the completion of individual Armistice agreements among the new state of Israel and the participating Arab nations. In comparison to the Second World War, a large-scale conflict that claimed 60 million lives, military operations in Palestine seem a relatively modest affair. After all, World War II was a total war in terms of proportion, participants, cost, and global impact. However, as author Efraim Karsh put it, "If anything, the Palestine War demonstrates that there is more to armed conflict than the size of the armies engaged in combat operations or the nature of their equipment."[3] To be sure, the War for Palestine *was* a large-scale war—but of a type and myriad complexity that defies single-narrative description.

At once, the War for Palestine was a British proxy war covered in the fingerprints of Britain's messy colonial-economic policies. It was an ideo-

logical war defined by the Zionist movement seeking a homeland for the Jews in Palestine. It was a theistic war informed by the Torah and the Bible that, according to God, "from the Negev wilderness in the south to the Lebanon mountains in the North, from the Euphrates River in the East to the Mediterranean Sea," it was promised to the descendants of Abraham.[4] It was an aspirational war for European Jewry seeking a land of their own after Nazi Germany and their collaborators murdered six million European Jews as part of a systematic plan of genocide—the Holocaust. For Arab League states it was a war of national self-interest deceptively cloaked under a banner of pan-Arabism. For devout Muslims committed to the defense of the Al Aqsa mosque in Jerusalem it was a holy war. When the UN declared Israel a state on 29 November 1947 at the expense of the Palestinians who had been the majority for the previous 500 years, it became a civil war. This was also an information war of competing historic, political, social, and religious narratives and propaganda. And last but not least, the War for Palestine was a large-scale land war fought on the ground by conventional and unconventional combatants.[5] Given such circumstances, how could any military officer involved in such a conflict possibly understand the situation? Such was the state of affairs following the Battle of Der Suneid in Palestine on 19 May 1947, that a canny Egyptian major named Gamal Abdel Nasser remarked "What kind of war was this?"[6]

When the ground war began in November 1947, six Arab Nations committed a token force of approximately 20,000 largely symbolic Arab troops to the "frontier" of Palestine with initial Jewish forces (regular and irregular) numbering roughly 55,000.[7] As a combined force they were poorly trained and equipped, lacked effective command and control, and lacked unity of effort. While the combined domestic populations of the six Arab countries near Palestine far outnumbered the sizeable Jewish Community now living in Palestine, the Arabs never mobilized and massed their available military strength for war in Palestine like the Jews. But why? Some scholars have suggested the Arab leaders cared less for the Palestinians themselves and were more interested in their own territorial ambitions. A 2010 *New York Times* Op-Ed by Professor Efraim Karsh of King's College of London stated:

> The first secretary-general of the Arab League, Abdel Rahman Azzam, once admitted to a British reporter, the goal of King Abdullah of Transjordan "was to swallow up the central hill regions of Palestine, with access to the Mediterranean at Gaza." The Egyptians would get the Negev. Galilee would go to Syria, except that the coastal part as far as Acre would be added to the Lebanon.[8]

During the course of the war Israel gained statehood via UN Resolution 181. Israel's "right of return" immigration law facilitated a significant influx of fresh military-age citizens, with priority given to those with combat training or experience from WWII. The Arabs never came close to matching Israel in terms of troop strength even when factoring in irregular forces of both sides. At its peak, approximate total number of combatants for each side were 17,500 Jewish fighters and 51,100 Arab.[9] Sixty-nine years later, the question of Palestine has not been resolved.

From the literature review, the majority of the available English-language scholarship on the 1948 War for Palestine concentrates on precipitating social-political-religious factors and major military offensives. Less

Figure 5.1. Majority report from United Nations Resolution 181. Map created by Army University Press.

represented in the available literature is scholarship dedicated to understanding the role of information in this conflict. This chapter contributes to the existing scholarship by exploring information as a function of national power and military warfare as seen by: (1) a sampling of the war's master narratives, and (2) a selection of the information products and programs used to influence public behavior and opinion. Call-out boxes throughout this chapter identify lessons learned to assist US military leaders in future Large-Scale Combat Operations (LSCO) of similar complexity.

Master Narratives of The 1948 Palestine War

Halverson, Goodall, and Corman define a master narrative as "A trans-historical narrative that is deeply embedded in a particular culture."[10] The War for Palestine was shaped, in part, by master narratives. These stories of strategic importance were crafted and employed by both sides and were used to rally key publics at home and abroad, foster unity-of-effort, differentiate friends from foes, and so on. But why should narratives matter to military leaders responsible for prosecuting ground wars of large scale? In his paper titled "The Military Application of Narrative: Solving Army Warfighting Challenge #2," published in 2016, Major Robert Payne III suggests, "The US Army has a problem. This problem is made evident by 14 years of sustained combat and no victory in sight. The problem is that the Army lacks any significant means of engaging its enemy where the enemy is fighting, namely, in the narrative space."[11] He further states, "The narrative space has always existed within warfare. The difference today is that western societies are adamantly opposed to the violence caused by war since WWII and in representative governments the passion of the people impact the conduct of the war."[12]

The following section will sample key master narratives put forth by the Zionists and the Arabs in the War for Palestine while highlighting lessons learned for military leaders in LSCO.

At the beginning of this chapter, Major Nasser of Egypt was quoted as asking "What kind of war was this?" The Zionist leaders and politicians sought to answer such a question using master narrative language to play on Jewish emotions, hopes, dreams, and fears. The concept of "total war" and the perception of the Palestinian "home front as a war front" were major elements of the Zionist narrative for the 1948 War.[13] While conventional military scholars would agree that the war for Palestine does not constitute a "Total War," Zionists relied on such language for military

mobilization. Author Moshe Naor describes how key Jewish leaders misrepresented the War for Palestine:

> The political leaders who served this function were David Ben-Gurion—the head of the Jewish Agency executive, and after May 1948 the first prime minister and minister of defense of the State of Israel—and Eliezer Kaplan—the treasurer of the Jewish Agency and the first finance minister of the State of Israel—who repeatedly used the concept of "total war" and the perception of the home front as a war front. Ben-Gurion and Kaplan expressed in the course of the war the importance that they, as the political leadership, ascribed to the mobilization of society and the support of society in the war effort. Ben-Gurion and Kaplan strove to stress as part of their mobilization rhetoric that the home front and the economy were an additional front in the war, and that the home front was no less important than the military front. Thus, on 13 November 1948, Ben-Gurion explained that: "this year we stood confronted by a total war. Everything was harnessed and mobilized on behalf of the requisites of the war—manpower, arms, capital, knowledge; because everything stood in jeopardy."[14]

In the beginning of the conflict, the Arab master narrative was based on notions of Pan-Arab strength and unity. The language evoked exaggerated notions of capability and intent. This narrative functioned as a strategic deterrent-of-sorts through the idea of the inevitability of Arab victory in any confrontation. As the actual conduct of the War for Palestine turned sharply in favor of the Jews, the Arab narrative changed to reflect a blame-and-shame posture. This version of the Arab master narrative evoked betrayal by the British who reneged on the McMahon-Hussein agreement and abandoned their mandate in Palestine. The Arabs cast the UN in a shameful light for their decision to create the state of Israel. The blame-and-shame narrative was a face-saving measure to cover the string of Arab military defeats by Jewish forces. The Pan-Arab narrative explains why at the outset of skirmishes in 1947 the Arab military actions were largely defensive in nature. Their primary purpose early on was to protect local Palestinians and Arab military personnel from the actions both from the Jew's conventional pre-state Army and Haganah irregular Jewish forces. Early on, the average Arab soldier and officer had every reason to be optimistic.

This passage from Major Gamal Nasser captures well the sentiment of the Egyptian soldier and state in April 1948:

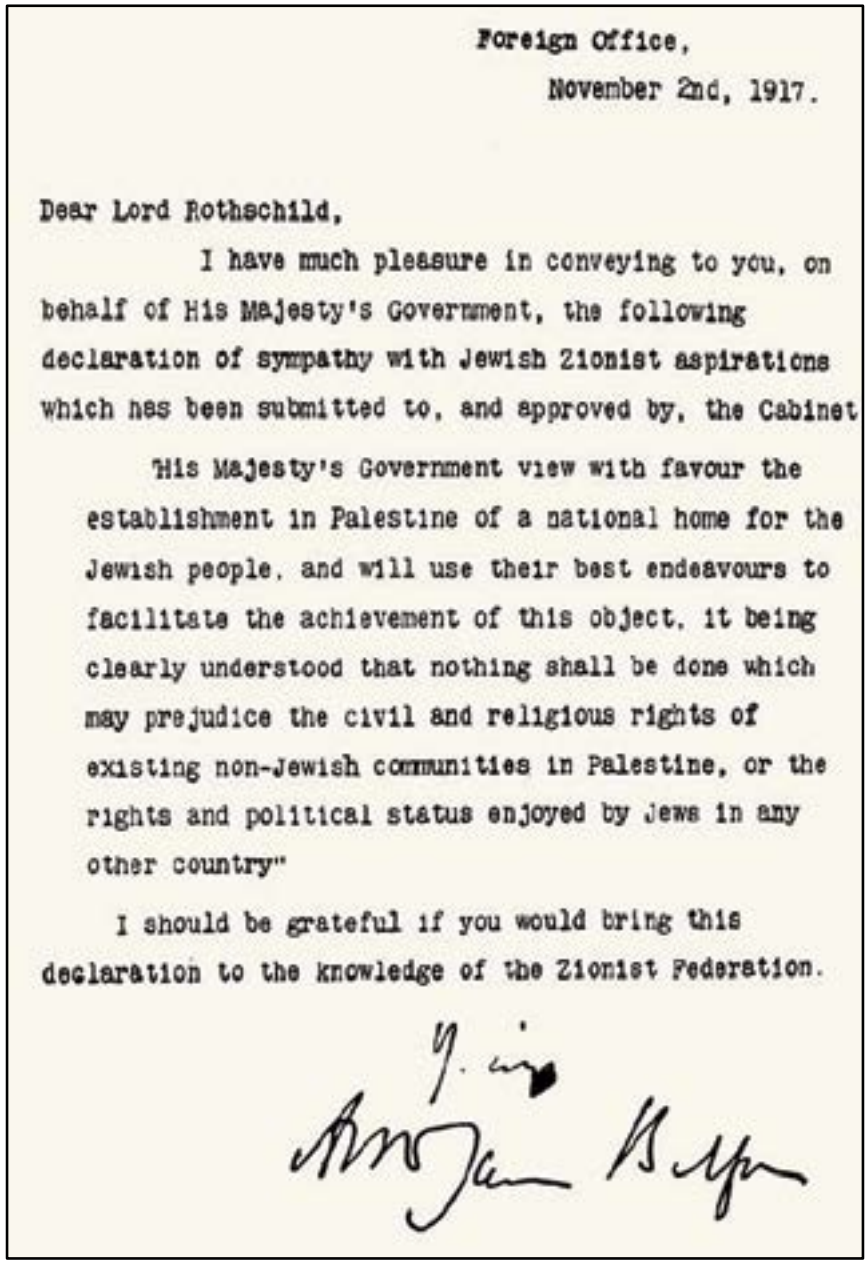
> I myself was engaged in completing my studies at the Staff College. But the worries and responsibilities of my work at the College could not shut out the sound of the war-drums in Palestine. There was a great deal of excitement among my colleagues and the morale, especially among the younger officers, was high. . . . The morning papers were full of news of what was happening in Palestine. At the same time there were various forecasts and conflicting reports as to the official stand that the Egyptian government might take on the subject. There was no specific indication in the papers as to what this stand might be. But it was beginning to appear that there was a possibility of our entering the Palestine war, and the general atmosphere in the country was overflowing with excitement.[15]

The optimism of the Egyptians was based on a false premise. Through government control of their national media, Egypt and other Arab League states attempted to conceal the military defeats that had occurred throughout the conflict and later polling suggest that 79 percent of the Egyptian population believed Egypt had won the war.[16] From the sample analysis of master narratives of the warring factions, one can see that the Israelis and the Arabs had different and often conflicting versions of actual events. History shows that "memory becomes shorter, patience diminishes, and propaganda competes successfully with historical knowledge."[17]

LSCO Lesson Learned #1

Identify the Master Narratives in play. Ensure you and your staff understand the crucial role they can play in achieving political and military objectives in LSCO.

Figure 5.2. Large-Scale Combat Operations Lesson Learned #1. Created by Army University Press.



Foreign Office,

November 2nd, 1917.

Dear Lord Rothschild,

I have much pleasure in conveying to you, on behalf of His Majesty's Government, the following declaration of sympathy with Jewish Zionist aspirations which has been submitted to, and approved by, the Cabinet

"His Majesty's Government view with favour the establishment in Palestine of a national home for the Jewish people, and will use their best endeavours to facilitate the achievement of this object, it being clearly understood that nothing shall be done which may prejudice the civil and religious rights of existing non-Jewish communities in Palestine, or the rights and political status enjoyed by Jews in any other country"

I should be grateful if you would bring this declaration to the knowledge of the Zionist Federation.

Yours sincerely,

Arthur James Balfour

Figure 5.3. “Balfour Declaration” letter from Sir Arthur Balfour to Lord Rothschild. Photo courtesy of the British Library.

Weaponizing Information: Key Documents and Radio in the British Mandate

The 1948 War for Palestine was informed and influenced by a range of strategic and operational information products—propaganda to some. Information Operations (IO) played a critical role in this war. This section will focus on a sample of key documents and radio programs in the former British Mandate to show how information was weaponized to meet British, Zionist, and Arab goals.

On 2 November 1917, British Foreign Secretary, Arthur Balfour sent a letter to Lord Walter Rothschild, a wealthy British-Jewish banker and financier of the Jewish cause. The letter (Balfour Declaration) had no legal binding but conveyed a message to the Zionist movement on behalf of the British government. It was this letter that allowed the Zionist campaign to claim that it was not just their hope and need for a Jewish state; now publically Britain supported their goal.

The impact of this state-sponsored document had a strategic effect on the League of Nations. On 24 July 1922, the Council of the League of Nations formalized the British government's role in Palestine. The preamble stated the Principal Allied Powers agreed with the Balfour Declaration, and that the British Mandate was responsible for putting into effect what has become known as the Balfour Declaration of 1917. Article 2 echoed the preamble and also required that the Mandatory: "be responsible for placing the country under such political, administrative and economic conditions as will secure the establishment of the Jewish national home . . . and the development of self-governing institutions, and also for safeguarding the civil and religious rights of all the inhabitants of Palestine, irrespective of race and religion."[18]

The formal Mandate gave Britain responsibility in seven areas. Article 3 gave instructions ensuring Jews would maintain a place to migrate to and establish a national home. Article 5, limited the ability of a foreign government to take control; Articles 9, 13-16, aimed to ensure religious rights and holy sites of all faiths were not restricted. Absent from the Mandate was guidance to how the Arabs of Palestine should be treated or guaranteed a national home of their own. The British Mandate of Palestine was a key moment for Jews and Arabs.

Nostalgia among the greater Jewish diaspora to return to its biblical home had existed for ages. Hence, the Balfour Declaration was a form of Strategic Information Operation made manifest. The Zionist-led cause for a Jewish homeland had found a patron in the world's leading power—

Britain. Thus the Balfour Declaration and subsequent policy action by the League of Nations in 1922 gave formal impetus and motivation for the creation of an Israeli state in Palestine. More important, this statement on behalf of the British government served as a successful propaganda tool in getting Jewish people from around the world to resettle, legally and illegally, in Palestine. The proof is in the numbers: the Jewish population was 70,000 in 1917 and 750,000 in 1948.[19]

Statements on both Arab and Jewish sides were used to influence their publics toward or away from conflict. On 11 October 1947, Abdel Rahman Azzam Pasha, Secretary-General of the Arab League, gave an interview in the Egyptian Arabic daily newspaper Akhbar al-Yom. His translated statement from the interview reads, in part: "I personally wish that the Jews would not work hard to push us to that war, because it will be a genocidal war which will cause great destruction and a lot of killing. History will record it like the killing that occurred during the Tatar times and the crusades."[20]

Azzam was seeking to de-escalate notions of war by emphasizing its terrible cost—this was clear in the original Arabic version. Azzam's quote was first modified and distributed by Zionist proponents and Jewish supporters in the press to resemble the following quote: "History will record it like the killing that occurred during the Tatar times and the crusades. . . . I am concerned about the coming bloody war. I can see its horrible battles; I can imagine a lot of fighting, killing, and wounded."[21]

In early 1948, the Jewish Agency submitted a memorandum to the UN Palestine Commission that significantly changed General Azzam's quote in meaning and context. Their submission to the UN quoted Azzam as saying: "This," he said, "will be a war of extermination and a momentous massacre which will be spoken of like the Mongol massacres and the Crusades."[22]

LSCO Lesson Learned #2

Know the political terrain. Strategic public correspondence, declarations, speeches, etc., can have operational and tactical implications for the Warfighter. To avoid operational surprise, stay informed about them.

Figure 5.4. Large-Scale Combat Operations Lesson Learned #2. Created by Army University Press.

Azzam's quote was purposefully changed to discredit the Arabs and generate support of the Zionist call for a UN decision favorable to the Jewish people. What Azzam actually said was now irrelevant as the truth and what some believed was the truth became blurred. This sigular informational effect propogated by the Jewish Agency had succeeded in damaging the credibility of Azzam and the intentions of the Arabs with a few strokes of the editor's pen. This disinformation effort, that presented a false account of history, has had a lasting impact: Google lists 395 books that include Azzam's altered quote excerpt and another approximately 13,000 websites that refer to it.[23]

The doctored quote became the perceived truth over time. The two changes referenced above show how a non-state actor like the Jewish Agency, using the power of information, can decisively change perceptions simply through the manipulation and usurpation of a rival narrative. In effect, the Jewish Agency was successful in garnering sympathy for the Jewish people and painting the Arab League as bloody-minded dervishes, but at the expense of the facts at the time.

Clandestine and National Radio Influences the Population

Though print news media was king in the early 20th Century, the 1920s saw a rise in amateur and private radio stations. "Technical advancements and an increased awareness of the 'power of radio' to reach and influence people had turned governments around the world into eager players, ready to transform broadcasting into a vehicle for serving state objectives."[24]

When the British government began its plans to start a state-sponsored radio service in its Palestinian mandate, they revoked local licenses and in turn removed competition to their own "Palestine Broadcasting Service."

LSCO Lesson Learned #3

Truth and deception are powerful weapons in war. Truth can be rendered irrelevant by ones' adversaries. Leaders at all levels should be thoughtful and judicious in the use of deception: for every deception, there are costs to maintain it.

Figure 5.5. Large-Scale Combat Operations Lessons Learned #3. Created by Army University Press.

With dominance of the local airwaves in mind, the British established the Palestinian Broadcasting Service (PBS) on 30 March 1936. PBS was headquartered in Jerusalem with the main transmitter in Ramallah. Other PBS transmitters were established at key locations areas across Palestine. In response to this restriction, the Zionist movement made great efforts to establish and produce its own clandestine radio operations. Lawrence Soley, Communications Professor at Marquette University, defined clandestine radio operations thus: "Illegal political stations that advocate civil war, revolution, or rebellion and provide misleading information as to their sponsorship, transmitter location, or *raison dêtre*."[25] During World War II, the potential of radio and radio operations during warfare had been fully realized. Just as it had in the Second World War, Radio operations would become a key feature of the War for Palestine.

For Arab League nations like Egypt, national radio outlets were weapons of informational power to be wielded in the battle for public opinion preceding, during, and after during large-scale combat operations. Such information operations targeted Egypt's enemies as well as its own citizens with the truth frequently being misrepresented to suit Egyptian national objectives. The below excerpt from memoirs of Gamal Abdel Nasser, then a major in the Egyptian Army and deployed to Palestine, underscores this point:

> I followed the developments of the battle of Deir Suneid from my position in Gaza, minute by minute. I could hear the boom of the guns in the distance. Our wounded started arriving in batches at Gaza Hospital. That night, the night of May 19, was the worst in my life. I spent it at Gaza Military Hospital. The beds around me were filled with our wounded from the battle of Deir Suneid, which was still in progress. Meanwhile Cairo Radio was announcing an official communique issued by General H.Q. [headquarters] in which our forces were said to have occupied Deir Suneid, which our infantry had stormed in a splendid manner. The communique contained a painful lie, for our forces had not yet occupied the settlement, though it was true that our infantry had carried out a splendid attack.[26]

When it became clear that the UN would recognize Israeli statehood sometime in 1948, the British began retrograde operations from their Mandate. The British plan for administrative continuity and uninterrupted service of PBS fell apart as British forces departed the country leaving powerful radio production and dissemination capability in the hands of the

two warring factions—Jews on one side and Arabs on the other. Regarding the fate of PBS following British retrograde:

> The station's footprint remained: the buildings and transmitter were still there and continued to broadcast on the same frequency, but the station's name, identity, and personnel changed. Physically, the station split: the broadcasting house, located in West Jerusalem, ended up in Israeli hands; the Ramallah transmitter, which had been taken by the Arab Legion, came under Jordanian control.[27]

The Haganah, and the stream of legal and illegal Jewish immigrants coming into Palestine, quickly assimilated this additional radio capability into their existing radio arsenal to further their objectives and to counter the relative advantage of neighboring Arab states national radio capabilities.

Under the British Mandate period from 1922–1948, unauthorized radio transmissions resulted in fines and punishment(s). Clandestine radio stations of both Arabs and Israelis had to be mobile and moved without notice. "Haganah Radio was the most extensive and well-organized of the Jewish clandestine radio services."[28]

LSCO Lesson Learned #4

In LSCO, prioritize information operations early. Whoever achieves and maintains relative information advantage over their opponent gains a significant asymmetric edge.

Figure 5.6. Large-Scale Combat Operations Lesson Learned #4. Created by Army University Press.

The utility of radio operation in Palestine in the War for Palestine was also tactically expedient. In 1947, approximately 60 percent of Arabs in Palestine were illiterate.[29] Radio was an ideal way to quickly reach a mass audience. The Haganah also understood what motivated their Arab enemies: "Arabs . . . are highly conscious politically . . . and are greatly swayed by editorials."[30] The Haganah took advantage of this:

> To this end, one tactic they used was to start a nightly Arabic news broadcast at 8:45 p.m. The broadcast covered "information" about individual Arab leaders, their "corruption," and "facts" about their embezzlement of public funds. The station would broadcast warn-

ings to individual Arabs (some of whom took these warnings very seriously and escaped to Egypt), and gave "inside information" on the situation "behind the Arab lines"—all designed to facilitate the ultimate achievement of Zionist objectives in the War.[31]

Figures 5.7 and 5.8 illustrate the extensive major radio and print programs in Palestine along with their attributable sources.

Name	Est.	Owned	Policy	Circulation	Significance/Audience
Palestine Broadcasting Service	1936–48	Mandate		103,090 sets in Palestine	Sets were subsidized; Listening licenses were $4 a year; Primary source for news, opinion, cultural influence approved by the British Mandate; Broadcast in English, Arabic, and Hebrew.
BBC			British entertainment		Clear reception was attainable in Palestine.
JCPA		British Military			Relayed BBC news.
Near East Broadcasting Corporation		British Foreign Office	Anti-Jewish		Composed of local Arabs (educated in Beirut); 1–2 Egyptians; Broadcast in Arabic.
Voice of the Revolution		Palestinian Arab	These radio stations operated with the intent to achieve their supporters' organizational goals and vision through the use of radio.	All listed radio stations other than PBS, JCPA, NEABC operated as clandestine radio stations.	
Voice of Palestine		Palestinian Arab			
Al-Inqaz Radio/New Arab "Secret" Radio		Arab Liberation Army			
Azerbaijan Democratic Station		Azerbaijan Democratic Party Tudeh Party			
Haganah Radio/Voice of Israel/Voice of Galilee		Haganah Army			
Voice of the Jewish Spearhead/Radio of Fighters for the Freedom of Israel		Stem Gang (LEHI)			
Voice of Fighting Zion/Voice of Freedom		Irgun			
Station of Arabic Prisoners of War		Israeli Army			
Free Jewish Station		General Zionist Council			

Figure 5.7. Survey of Major Radio Programs in Palestine 1948–1950. Created by Army University Press.[32]

Name	Est.	Owned	Policy	Circulation	Significance/Audience
Haheruth	1908–18	Hebrew			1st Palestinian Hebrew Daily
Moriah	1909–18	Hebrew			
Falastin	1911	Christian	Nationalist	~20,000	Muslim and Christian Arabs
Haaretz	1918	Hebrew	Pro-Zionist	~17,000 in 1940, Increased post-WW II	Liberal
Official Gazette	1919	Mandate	Pro-British		Published legal, municipal, and civil service notices; Weekly government publication.
Davar	1925	Hebrew	Socialist/ Labor	~32,000; ~35,000	TA: Co-op, women, and male working population.
Ad Difa'a	1932	Muslim	Nationalist	>10,000;~1,000	Muslim and Christian Arabs.
The Palestine Post	1925, 1932	Jewish	Pro-Zion		Now The Jerusalem Post; English, main story on the right side in an "American Style;" Opposed British immigration restriction.
Palestine Illustrated News	1933	Jewish			English, main story on the right in a "British Style."
Haboker	1935	Hebrew	Right-Wing	down to~13,500 by 1950	Two signers of Israeli Declaration of Independence.
Esh-Shaab		Muslim			Muslim, backed by Mussa El Alami (politician).
Al Wahdah		Muslim			Muslim, ed. Ishak Husseini (uncle al-Husayni).
Various	Hebrew daily papers: A revisionist, liberal farmer, two religious specific, and a German daily paper for recent immigrants (Hebrew and German).				
Immigrant Specific	Two German daily papers for those that did not learn Hebrew.				
Gazetta Polska		Refugee	TA: Polish refugees		Published by Polish refugees who stayed after WW II.
London Communist Daily Worker			Communist		Russian paper banned by the Mandate government.
Forum (English)	Early years of WW II	Public Information Office	Pro-British		Palestine Broadcast Service and BBC programs; Literary, Informational, and Poetry.
Hagalgal (Hebrew)			Pro-British		
Al Kafila (Arabic)			Pro-British		

Figure 5.8. Survey of Major Print Programs in Palestine 1909–1950. Created by Army University Press.[33]

Conclusion

In conclusion, the 1948 War for Palestine remains a fascinating academic subject with a complexity that belies its modest size and duration. It also gives insight to the political realism of the day. For those ground combat professionals seeking insights from historic LSCO, the War for Palestine offers maneuver commanders and staffs a useful framework for understanding and employing information operations. Three critical implications for the warfighter are presented here.

First, *informational power **is** power* as seen in the examples of the establishment of the Zionist movement in 1897, the Balfour Declaration in 1917, and the UN Resolution 181 in 1947. Given this perspective, one could deduce that the War for Palestine was a logical extension of these three informational efforts. In such a war as this, how could any ground commander fully appreciate the battlefield conditions without the context of the Zionist movement's objectives, the purpose of the Balfour Declaration, or the implications of UN resolution 181? This is a teachable moment for the modern day Army officer: if the purpose of war is to make conditions for a lasting peace, one must understand the pre-existing historic, informational, anthropologic, and political factors bearing on the military problem.

The second critical implication of this study contends that *information operations are a component of combined arms operations*. This point is illustrated in the example of the Jewish Agency and how it successfully corrupted and usurped Abdel Rahman Azzam Pasha's words, and subsequently, the Arab League's narrative. Doctrinal terms matter here. Joint Publication 3-0 defines an *operation* as "a sequence of tactical actions with a common purpose or unifying theme."[34] Joint Publication 3-13 defines *Information Operations* as: "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[35]

The Jewish Agency had a clear end-state in mind: to assist in securing a future Jewish state by encouraging Jews throughout the world to help in the development and settlement of Israel. The literature suggests the Jewish Agency's task and purpose was to exploit their political connections, resources, and access to print and radio media to disseminate a false narrative attributed to Azzam Pasha and the Arab League. The effectiveness of the Jewish Agency's political information operations highlights the power that civil-society organizations can have on the context, conduct, and mo-

tive of and for armed conflict. In this case, the Jewish Agency successfully discredited Azzam Pasha and the Arab league in a masterstroke of planned propaganda. So compelling was the Jewish Agency's propaganda campaign in 1948, that as of 2018, 395 books and 13,000 websites quote the altered Jewish Agency language given to the UN and attributed to Azzam Pasha as fact. While the Jewish Agency was successful in their efforts, this "tactical" action serves as a cautionary tale of the strategic impacts of tactical deception operations. It further underscores the need for LSCO to be guided and informed by a higher deception plan that considers long-term consequences of deception operations.

The third and final implication of this study maintains that *maneuver in the information environment **is** maneuver* as evidenced by Arab and the Israeli Forces' extensive print and radio operations. Joint Publication 3-0 *Operations* states that maneuver is "the employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy."[36] Consider the two illustrations of major print and radio programs included in this study. That such a relatively minor war could have been defined by such a contested information environment is staggering when one considers what this means for contemporary armed conflict. In 1948, both sides vied for advantage of the information terrain via information operations. Both sides used information operations to generate combat power by synchronizing available information capabilities. Today, with the internet-of-things, mobile wireless devices, instantaneous self-publishing software, drones, artificial intelligence programs, micro-satellite deployment, and big data operations, the information environment has become exponentially more complicated. Planning, coordinating, and synchronizing operations in the information environment requires more than a Ranger Tab. IO requires committed intelligence support, a detailed appreciation of how human beings interact within the information environment and with another; it calls for knowledge of the full range and application of available information-related capabilities (IRCs); it also calls for fluency in the operations process in order to turn the raw potential of informational power into combat power. It is likely that the next LCSO involving American troops will be every bit as complex as the 1948 War for Palestine. Regardless of the type of war it is, it will include, and quite possibly be defined by, a highly-contested battle for the information environment as it was in the case of Palestine in 1948.[37]

Notes

1. George Catlett Marshall, "The Time Factor: September 1–December 31, 1939," in *The Papers of George Catlett Marshall, We Cannot Delay*, 1 July 1939–6 December 1941, eds. Clarence E. Wunderlin, Sharon R. Ritenour, and Larry I. Bland, Vol. 2. (Baltimore and London: Johns Hopkins University Press, 1986), 123.

2. Donald Neff, "Preface: The Six Pillars of U.S. Policy, 1897–1995," in *Fallen Pillars: U.S. Policy towards Palestine and Israel since 1945*, ed. Eric Hoogland. (Washington, DC: Institute for Palestine Studies, 2002), 1–2.

3. Efraim Karsh, "Perpetuating the Arab-Israeli Conflict," in *The Arab-Israeli Conflict: The Palestine War 1948*, ed. Robert O'Neill, (Oxford: Osprey, 2002), 87.

4. "Possessing the Land" in *Holy Bible: New Living Translation*, 3rd ed., (Tyndale House Publishers, 2007), 336.

5. "Timeline of Events: After 1945," United States Holocaust Memorial Museum, accessed 24 April 2018, https://www.ushmm.org/learn/timeline-of-events/after-1945.

6. Gamal Abdel Nasser, "Nasser's Memoirs of the First Palestine War," translated by Walid Khalidi. Journal of Palestine Studies 2, no. 2, Winter 1973, 12.

7. Central Intelligence Agency, "The Palestine Situation 1948," 1–3, accessed 14 April 2018, https://www.cia.gov/library/readingroom/document/cia-rdp67-00059a000200200011-5.

8. Efraim Karsh, "The Palestinians, Alone," Editorial, *New York Times* (London), 1 August 2010, accessed 10 March 2018, https://www.nytimes.com/2010/08/02/opinion/02karsh.html.

9. Avi Shlaim, "Israel and the Arab Coalition in 1948," in *War for Palestine: Rewriting the History of 1948*, eds. Avi Shlaim and Eugene L. Rogan. (Cambridge, United Kingdom, Cambridge University Press, 2007), 79–103; Central Intelligence Agency, "The Palestine Situation 1948."

10. Jeffry R. Halverson, Steven R. Corman, and H.L Goodall Jr., "What Is a Master Narrative?" in *Master Narratives of Islamist Extremism* (Basingstoke: Palgrave Macmillan, 2011), 14.

11. Robert D. Payne III, "The Military Application of Narrative: Solving Army Warfighting Challenge #2," technical paper no. AD1020344, US Army Command and General Staff College, 2016, accessed 23 April 2016, http://www.dtic.mil/dtic/tr/fulltext/u2/1020344.pdf, iv.

12. Payne, "The Military Application of Narrative."

13. Moshe Naor, "Israel's 1948 War of Independence as a Total War," *Journal of Contemporary History* 43, no. 2, 1 April 2008, 242.

14. Moshe, "Israel's 1948 War of Independence as a Total War."

15. Nasser, "Nasser's Memoirs of the First Palestine War."

16. Yoav Gelber, “Israel Studies an Anthology: The Israeli-Arab War of 1948,” Jewish Virtual Library: A Project of AICE, July 2009, accessed 4 May 2018, http://www.jewishvirtuallibrary.org/jsource/isdf/text/gelber.pdf.

17. Gelber, “Israel Studies an Anthology.”

18. Lillian Goldman Law Library, “The Avalon Project: The Palestine Mandate,” The Avalon Project: The Palestine Mandate, 2008, accessed 27 March 2018, http://avalon.law.yale.edu/ 20th_century/palmanda.asp.

19. Leslie John Martin, “Press and Radio in Palestine under the British Mandate,” Journalism Bulletin 26, no. 2, 1949, 186.

20. David Barnett and Efraim Karsh, “Azzam’s Genocidal Threat,” Middle East Forum, 1 September 2011, accessed 15 May 2018, https://www.meforum.org/articles/2011/azzam-s-genocidal-threat. Original newspaper article was translated by a Command and General Staff College student and foreign officer.

21. Barnett, “Azzam’s Genocidal Threat.”

22. Jewish Agency for Palestine, Memorandum on Acts of Arab Aggression to Alter by Force the Settlement on the Future Government of Palestine Approved by the General Assembly of the United Nations: Submitted to the United Nations Palestine Commission, Jewish Agency for Palestine, 1948, 3, accessed 27 March 2018, https://archive.org/stream/ MemorandumOnActsOfArabAggressionSubmittedToTheUnitedNationsPalestine/ MAAA2#page/n19/mode/2up/search/Pasha.

23. Tom Segev, “The Makings of History: The Blind Misleading the Blind,” *Haaretz.com*, 11 January 2018, accessed 27 March 2018, https://www.haaretz.com/1.5201895.

24. Andrea Stanton, “Jerusalem Calling: The Birth of the Palestine Broadcasting Service,” *Jerusalem Quarterly* 26, no. 50, 2012; The Institute for Palestine Studies, accessed 5 April 2018, http:// www.palestine-studies.org/jq/fulltext/78483.

25. Lawrence C. Soley, *Radio Warfare: OSS and CIA Subversive Propaganda*. (New York: Praeger, 1987), 2.

26. Nasser, “Nasser’s Memoirs of the First Palestine War.”

27. Stanton, “Conclusion: The Multiple Afterlives of PBS.”

28. Douglas A. Boyd, “Hebrew-Language Clandestine Radio Broadcasting During the British Palestine Mandate,” *Journal of Radio Studies* 6, no. 1, 1999, 102.

29. Martin, “Press and Radio in Palestine,” 187.

30. Martin, 192.

31. Martin, 192.

32. Lawrence C. Soley and John S. Nichols, *Clandestine Radio Broadcasting: A Study of Revolutionary and Counterrevolutionary Electronic Communication* (New York: Praeger, 1987), 320; Martin, “Press and Radio in Palestine under the British Mandate;” Douglas A. Boyd, “Hebrew-Language Clandestine Radio Broadcasting During the British Palestine Mandate,” *Journal of Radio Studies* 6, no. 1, 1999, 102.

33. Martin, “Press and Radio in Palestine,” 186.

34. Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Personal Support* (Washington, DC: 2017), GL-13.

35. Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: 2012 w/ Chg 1 2014), GL-3.

36. Joint Chiefs of Staff, Joint Publication (JP) 3-03, *Operations* (Washington, DC: 2012), GL-12.

37. Major H.O. Lock, "Contents," in *The Conquerors of Palestine through Forty Centuries*, ed. V. London: R. Scott, 1920, accessed 14 March 2018, https://archive.org/details/; Chaim Weizmann, *Trial and Error: The Autobiography of Chaim Weizmann* (New York: Harper, 1949), 149; Ministry for Culture and Heritage, "Palestine Campaign Map," Map in *The Oxford Companion to New Zealand Military History*, Oxford University Press, 2000, accessed 21 March 2018, https://nzhistory.govt.nz/media/photo/palestine-campaign-map.

Chapter 6

Leaflets and Loudspeakers: The Role of Psychological Operations (PSYOP) in Large-Scale Combat Operations

Lieutenant Colonel Andrew D. Whiskeyman

To seduce the enemy's soldiers from their allegiance and encourage them to surrender is of special service, for an adversary is more hurt by desertion than by slaughter.

—Flavius Vegetius Renatus, c. 378 AD

"We are in an information war, and we're losing that war," is an oft-repeated quote regarding the fight against Islamic extremists.[1] While it is not solely the responsibility of the US military to win this narrative, it is certainly incumbent on the US military to use information to gain a relative advantage over enemies in combat. The *raison d'etre* of the US Army is to win the nation's land wars. It should be obvious that this includes an element of information warfare because war is inherently a contest of will susceptible to psychological manipulation. This is especially important because information is now a joint function, and the US Army has recognized the growing importance of information on a multi-domain battlefield through the creation of an Information Dominance career field inclusive of cyberspace operations (CO), electronic warfare (EW), and information operations (IO) officers.[2]

The US military has struggled with grasping the nature of information operations. This is evident in the confused language often heard as the terms IO and Military Information Support Operations (MISO) are used interchangeably. While the two specialties are intimately related, there are key differences between them. IO officers integrate a broad range of information related capabilities, while PSYOP officers specialized in the development of messages designed to resonate with a given audience. MISO focuses on the message and the most effective delivery method to create a perception; IO focuses on the integration of the message with other activities. Additionally, information operations tend to be viewed as a necessary evil. IO are not a readily accepted practice within the Army because the perception that underhanded methods are employed is an anathema concept to an Americans sense of values-based fair play.

According to Susan Gough, the use of "'psychological tricks' is 'dirty' and immoral," and has been viewed as "something that only the 'bad guys' did: first the Nazis, then the Soviets."[3] This understanding of the nature of

information operations has often hindered an effective employment of the craft.[4] Information operations do not come naturally to the Army's staffs because it is not sufficiently emphasized within the Army's Leader Development, Education, and Training (LDT&E) processes that groom future staff officers and commanders. This appears to be evident in ongoing operations where one could argue that the US military has been successful in nearly every tactical engagement in Afghanistan, Iraq, and Syria, but cannot seem to gain the advantage in the psychological fight.[5] The enemy holds on. He does not quit. He bides his time. This is not a new problem, however. Recall that Napoleon—for all his acclaimed tactical brilliance—fought all the way to Moscow but failed to convince the Russians to quit. He lost the psychological war, and ultimately his tactical successes were for naught. So, how does a commander establish the necessary operational conditions to enable success in the IO fight?

Because it can be difficult to make assessments in the midst of action, a study of history can be informative. By examining key case studies from the past, one can draw out some universally applicable truths, which then can be applied to the current (and future) situations in hope that one does not repeat the mistakes of the past. The Vietnam War offers a fertile opportunity because to date, it was the largest use of psychological operations in US history.[6]

Because information operations as a term did not exist during the Vietnam War, this chapter will attempt to draw some conclusions by examining the use of psychological operations (PSYOP) (the term for MISO during the Vietnam War) during large-scale combat operations (LSCO) in Vietnam. The first aspect this chapter will examine is at Military Assistance Command Vietnam (MACV) headquarters. The second and third aspects to be examined occurred during the largest ground operation of the war (Operation Cedar Falls) and during the largest airborne operation of the war (Operation Junction City).

To conduct this analysis, this summary will briefly examine US Army doctrine on PSYOP during the period in question (1965–1967). Did the US Army have a firm footing upon which to build its PSYOP program? Next, each case study will be examined on three key criteria: command emphasis, resourcing, and metrics. Finally, this chapter will make some conclusions and recommendations for how the Army should conduct some facets of information operations during future LSCO based on the lessons learned from the employment of PSYOP during the Vietnam War.

Doctrinal Review

The US Army's first official doctrine dates from 1778—a time when the Continental Army was poorly trained compared to its adversaries the British Army and their Hessian mercenaries. Confronted with this dilemma, General George Washington sought assistance from Major General Friedrich Wilhelm von Steuben, who developed and published the *Regulations for the Order and Discipline of the Troops of the United States*, which became known as the "blue book." The manual remained the Army's official military guide until 1812.

From the time of the American Civil War on, the US Army developed field manuals (FMs) to cover specific aspects of warfare. The need for a larger standing Army post-WWII necessitated a continual refinement of the doctrine required to support the fielding, training, and equipping an industrial-age warfare force. Modern US Army PSYOP doctrine is rooted in WWII, with further refinement coming through the Korean War and the early years of the Cold War.[7] The result of that 25-year history of maturation was that the American Army entered Vietnam with a well-defined PSYOP doctrine.[8] While PSYOP doctrine was well-defined, it was not well integrated with intelligence doctrine as this tended to fixate on order of battle and not on the sorts of intelligence required to produce effective PSYOP.[9]

MACV leadership recognized the challenges of the fight in Vietnam. So, on 7 September 1965 it published Directive 525-3, "Minimizing Non-Combatant Battle Casualties," which built upon existing doctrine and sought to clarify the need to include the psychological aspects of warfare in ongoing and future operations.[10] The directive stated that "the use of unnecessary force leading to noncombatant casualties in areas temporarily controlled by the Viet Cong (VC) will embitter the population, drive them into the arms of the VC, and make the long range goal of pacification more difficult and more costly."[11] Annex A to Directive 523-3 directed commanders to integrate tactical psychological operations with civic action and combat operations. Commanders who failed to implement PSYOP and civic action in coordination with combat operations were thus not only ignoring doctrine, they were also ignoring General William Westmoreland's orders.[12] Unfortunately, officers arriving in Vietnam had little to no PSYOP training. The US Army's yearlong command and general staff college (CGSC) focused on the tactics of fire and maneuver and only taught one hour of PSYOP curriculum during the entire year. Despite Westmoreland's emphasis, the officers arriving to Vietnam lacked the training on

how to execute his orders effectively. MACV had the requisite command emphasis but did not have the training to put it into practice.

PSYOP at MACV

By mid-November 1966, this expanded command emphasis placed a demand on PSYOP resources that outstripped capacity. So, the decision was made that the 6th PSYOP Battalion would be expanded to a group and that staffing levels within the MACV headquarters would be increased.[13] Additionally, all maneuver battalions were also to be issued hand-held loudspeakers based upon a suggestion of then Lieutenant Colonel Hal Moore, who had argued that each brigade should receive its own loudspeaker team.[14] MACV continued to learn, adjust, and improve its operations.[15]

This was also true with intelligence operations where several assessments led directly to changes in PSYOP tactics and messaging. Despite not having well-integrated doctrine, MACV as a command learned from ongoing operations and adjusted. Interrogation of enemy captives and *Hoi Chanh* (rallier in Vietnamese) produced assessments that meager rice rations and inadequate medicinal supplies had eroded VC combat effectiveness.[16] This analysis led to a focus on those themes in *Chieu Hoi* (open arms in Vietnamese) messages, which demonstrated coordination between the MACV J2 and the psychological operations community.[17] The *Chieu Hoi* Program was designed to encourage insurgents to abandon the VC and join in the building of South Vietnam as a nation. It also aimed to undermine community and family support for the insurgents by destroying the belief that friends and family were obliged to support any relatives in the insurgency.[18] It sought to accomplish these goals by providing job training, political indoctrination, and in some cases a basis for acceptance into the Army of the Republic of Vietnam (ARVN).[19] The military intelligence community published a detailed analysis of who the *Hoi Chanh* were and their likely reasons for defection. The US recognized that each *Hoi Chanh* was one less VC on the battlefield and that the costs of not embracing this program would be significant in terms of US lives lost.[20] One US estimate calculated the cost of each *Hoi Chanh* at $127, while the cost to kill each VC was $300,000.[21]

So MACV had relatively sound doctrine, command emphasis from General Westmoreland, and made resource allocations to support PSYOP. The crucial elements seemed to be present for successful psychological operations. The next aspect to be examined is how that framework was executed during LSCO.

Cedar Falls

Operation Cedar Falls began on 8 January 1967 and ended on 28 January 1967. It was the largest US ground operation in Vietnam and included the use of 30,000 US troops.[22]

The operation's purpose was to deny the enemy the use of the Iron Triangle: an area to the northwest of Saigon that the National Liberation Front (NLF) had used as an operations base since at least 1945. This area was about 155 square kilometers and had grown along with the increase in US troop commitment. By the time of Cedar Falls, the area was a "complex of cement fortifications, three-tier tunnel systems, ammunition depots, munitions factories, hospitals, troop rest and recreation areas, and communication centers."[23] Additionally, MACV intelligence assessed that significant enemy forces were operating in the Iron Triangle. These forces consisted of the NLF's Military Region IV headquarters, the 272d regiment, and five battalions of the 165th VC regiment. A local force battalion and three local force companies were also operating in the Iron Triangle.[24]

Two days prior to the start of the ground operations, PSYOP conducted a shaping operation by dropping 215,000 leaflets on the area that urged the populace to "go to designated assembly points for evacuation before the shooting started."[25] The goal was clearly not surprise. Instead, commanders sought to minimize civilian casualties and destroy the NLF structures so that they would no longer be able to use the area.

The use of tactical PSYOP teams was very effective. As the operation continued, the number of *Chieu Hoi* increased.[26] The PSYOP teams were able to exploit opportunities rapidly because they had the ability to operate at the lowest tactical level. They created "rapid reaction leaflets," which were a very effective means of motivating enemy personnel to defect.[27] These leaflets were often comprised of first-hand testimonials from enemy prisoners. This was an example of a multi-domain battle long before the phrase was coined. The Army and Air Force used combined arms to fix the enemy, while PSYOP used leaflets and loudspeakers to target him when he was most psychologically vulnerable. The result of this and other efforts was that over 500 VC rallied, or turned themselves into the Vietnamese government during Cedar Falls.[28] Post-strike reporting from B-52 strikes during Cedar Falls showed that the VC rallied due to the terror of the bombings and the use of leaflets and loudspeakers.[29] Interrogations and enemy document exploitation revealed that from the VC perspective, "psychologically speaking, the use of B-52's by the enemy for bombing, along with an extensive propaganda program considerably lowered the

morale of cadre and [the] mass[es]."[30] Additionally, many enemy units largely avoided contact and withdrew across the border into Cambodia. While this withdrawal cannot be directly attributed to PSYOP, it is likely that the combination of overwhelming firepower and the targeted use of tactical PSYOP created the conditions where the enemy sought to avoid contact.

Here again, the fundamental elements and conditions required for success were in place. Commanders placed emphasis on PSYOP (it led the operation), applied resources, and the efforts of PSYOP delivered results. The next operation serves as our second case study.

Junction City

At the close of 1966, based on captured enemy documents and interrogations of *Hoi Chanh*, the MACV J2, General Joseph McChristian, assessed that seven North Vietnamese divisions subordinate to the Central Office for South Vietnam (COSVN) operated in Military Region 5.[31] Based on this intelligence, he approached Westmoreland with an interesting proposition—that Westmoreland delay and significantly change an operation that was already set to commence. General Westmoreland trusted McChristian, and acting on that trust Westmoreland agreed to delay and change the planned operation.[32]

Junction City was a three-phased operation that began on 22 February 1967 and lasted 82 days. US Army and Air Force units, along with the support of the Army of the Republic of Vietnam (ARVN), fought against forces of the Viet Cong and North Vietnamese Army (NVA). This operation took place in the region known as War Zone C which was northwest of Saigon and just beyond the Iron Triangle—the area previously cleared during Cedar Falls.[33] Junction City covered an area of approximately 4,000 square kilometers about 45 miles northwest of Saigon and bordering Cambodia.[34] This operation built upon the successes of Cedar Falls and was designed to destroy the Central Office of South Vietnam (COSVN), which some analysts believed to be the VC equivalent of the Pentagon.[35]

Junction City was a search-and-destroy operation, which used more troops to cover a larger area than ever before and used more helicopters than any previous operation in the US Army's history. It was also the only major airborne operation of the Vietnam War. The mission of the II Field Force was to search and destroy COSVN and the 9th VC Division and their installations.[36]

The operation failed to find COSVN but did lead to the capture and destruction of a significant amount of VC materiel. The operation had sig-

nificant short-term tactical success but failed to secure long-term strategic results. That said, there were some notable PSYOP successes.

After the battle of Ap Bau Bang II, General John Hay, the 1st Infantry Division commander, wrote to his counterpart in the 9th VC Division and had the message printed and dropped into enemy areas. It stated that the 9th Division commander's men had disgraced themselves not only by losing the battle, but also by leaving their dead and wounded behind. General Hay stated that the Americans were taking care of the wounded and had buried the VC dead.[37] This command emphasis showed a willingness to engage with the enemy psychologically.

Another success came on 28 February 1967, when the 173rd Brigade operating northeast of Katum had a major find: 120 reels of motion picture film, numerous still photos and pictures, and busts of communist leaders. This discovery proved to be one of the major intelligence coups of the war.[38] The Combined Document Exploitation Center (CDEC) processed and analyzed the film, and then combined the analysis into 65 reels of varying lengths of five to 30 minutes. This collection was an enormous boon to the order of battle effort, as it provided visual identification of individuals in the VC hierarchy. It also had psychological operations value, leading the MACV J2, in cooperation with the Joint US Public Affairs Office (JUSPAO), to compile five of the films into a 35-minute composite with an English commentary.[39] Visually identifying individuals in the VC hierarchy prevented them from continuing to hide among the population. JUSPAO was also able to use some of the intelligence exploitation generated from operations such as Junction City, which could then be used to bolster support for similar operations in the future. MACV intelligence assessed that the identification of VC leaders demoralized their forces.

Junction City resulted in 139 *Chieu Hoi*. The lower results were assessed because the 9th VC Division was made up of North Vietnamese regulars and hardened VC, which meant the normal appeals to family separation were not as effective.[40] Junction City dropped 9,768,000 leaflets, and made 102 hours of aerial loudspeaker appeals, with most of the engagements in March resulting in quick reaction leaflets being created and distributed to take advantage of the developing tactical situation.[41]

As was the case in previous operations, the enemy avoided contact, and Soldiers were astute enough to recognize that the capture and exploitation of VC or VC propaganda presented a significant intelligence advancement in terms of identifying a previously faceless enemy. While there were not as many ralliers as during Cedar Falls, there were still a company's worth

of enemy combatants removed from the battlefield using PSYOP. As was the case in Cedar Falls, Junction City PSYOP efforts benefitted from command emphasis and resourcing which in the end produced results.

Conclusions

Cedar Falls and Junction City were the two largest ground operations conducted by the US Army during the Vietnam War. If those keystone operations were emblematic of MACV efforts, then one should have assumed that the US would have won the psychological war in Vietnam. MACV (and subordinate commands) had the key elements of success present: they placed emphasis on PSYOP, allocated resources, and sought to assess effects. Westmoreland briefed all incoming battalion and above commanders of the need for PSYOP and their role as the primary PSYOP officers in their units. Despite the unprecedented command emphasis, General Westmoreland only makes one mention of PYSOP in his autobiography, *A Soldier Reports*:

> Psychological warfare detachments operated throughout South Vietnam, distributing leaflets, broadcasting over loudspeakers, trying in various ways to persuade the enemy to defect . . . Yet despite a major and persistent effort, including bringing civilian psychological warfare experts from the United States, results were disappointing. Except for an occasional platoon-size group, most defectors were individuals. Mass surrenders never developed despite our intense psychological warfare efforts, which apparently could not overcome the enemy's intensive indoctrination.[42]

Westmoreland was clearly disappointed with PSYOP's performance. He expected immediate results, and when they did not happen, he blamed MACV for the ineffective employment of PSYOP. Yet, even though Westmoreland took a personal interest in PSYOP, a survey of lessons learned cited 17 of 21 battalion commanders that there was no requirement for psychological warfare personnel at battalion level, and only four commanders felt that psychological warfare personnel should be included in the battalion.[43] Additionally, the general attitude seemed to be that anyone could write a leaflet, which undermined the desire for the addition of PSYOP teams. The expectation was that someone else would take care of that fight—that real warriors used firepower and not "dirty tricks."

Many commanders interpreted MACV Directive 525-3 as if those functions were compartmented, rather than complementary. Thus, some units in Vietnam were also dividing the functions of PSYOP and Civil Affairs as two unrelated activities; failing to see the linkage between deeds

and words. Commanders viewed leaflet and loudspeakers as a type of fires, which could be measured, assessed, and would produce immediate results.

There were other instances where "commanders saw PSYOP as more of a sideshow than a valuable combat multiplier."[44] There is also the remark of one commander "who boasted that his Chieu Hoi program consisted of two 105mm howitzers—one of which was marked 'Chieu' and the other 'Hoi.'"[45]

The intelligence community also had systemic challenges with PSYOP support. While McChristian cited incidents of cooperation and support from intelligence to PSYOP, the 7th PSYOP Group report from November 1967 was not so sanguine. PSYOP personnel did not have access to the 3M Reader Printers needed for CDEC use. Thus, they were unable to mine that vein of intelligence.[46] Additionally, as late as mid-1967, both the 6th PSYOP Battalion and 7th PSYOP Group requested that MACV J2 place them on its distribution lists, but no action had been taken because the requests were not relayed to the correct section of the MACV J2.[47]

The study also found that PSYOP intelligence unit interrogators were not being granted access to military interrogation facilities.[48] PSYOP specialists were required because J2 analysts were consumed with the collection of order-of-battle information, and often either missed or ignored intelligence of psychological value.

Despite the command emphasis, success was not forthcoming during Vietnam. The largest use of psychological operations in US history had failed to deliver the expected results. The failure does not seem to rest at the tactical level, as units attempted to integrate PSYOP, learned lessons from ongoing operations, and adjusted tactics. The failure then is in expectation management. General Westmoreland did not understand the nature of psychological operations and placed the wrong sort of command emphasis on those operations. He unrealistically expected instantaneous results and believed that tactical level PSYOP could produce operational and strategic level effects.

Lessons for Today

Commanders today face similar challenges with MISO (i.e. previously PSYOP) and more broadly with the integration of non-lethal fires into the fight. Too often commanders view non-lethal fires writ large as a mechanism to mitigate risk from the fallout of tactical operations instead of viewing information warfare as the main point of conducting operations. Commanders are not expected to by MISO experts, but they should

have a solid grasp of how to integrate information related capabilities into plans and operations.

The point of warfare is to get one's enemy to capitulate. Unless the enemy is dead, the only other way to do so is to win the information fight. Yet, information operations is taught only as an elective at CGSC—not a very helpful fact when we are engaged in ongoing struggles with adversaries who plan the IO-effect first and then plan the tactical engagement. This is true of the fights with extremists as well as with the actions short of armed conflict with states such as Russia and China.

After all, the refrain of "we are losing the IO fight" still resonates within many headquarters. So, what is to be done? First, commanders must look inward to acknowledge, despite their experiences, they are not IO experts. Commanders must embody the mission command spirit and trust those that are experts to do their jobs.

Secondly, cultural barriers must be broken down that limit the optimal effectiveness of information-related capabilities. This starts with establishing the leader development training and education (LDT&E) processes within professional military education (PME) that places value on the employment of information related capabilities (IRC) in a multi-domain battle context. The IRCs must be taught within PME as more than just an elective—the core concepts must be infused in every lecture, reading, and exercise. Additionally, IRCs must be resourced with personnel, equipment, intelligence support, and office space. IRCs planners should be included in normal staff battle rhythm events and should be a priority when it comes to boots on the ground (BOG) requirements. IRC personnel are a vital part of the team and must be integrated within the commander's battle rhythm events.

Lethal and non-lethal fires must be part of the same commander's decision-making cycle. Too often, these are viewed as separate events. Further, intelligence must support IRCs. Most of the intelligence required by MISO comes from non-traditional sources that are outside of normal order-of-battle collection. Intelligence for IRCs must be prioritized. Fundamentally, the IO fight must be planned early. As seen during Cedar Falls, IRCs can be used to shape an operation. The use of IRCs should be proactive vice reactionary.

Finally, command emphasis is not a panacea. The commander must understand the nature of psychological warfare. Tactical MISO is very effective because the enemy is most vulnerable when he is faced with a multi-domain dilemma—when he has nowhere to turn for escape and

has lost hope. MISO above the tactical level does not produce immediate results. This is where the inclusion of MISO as part of information operations becomes vital. Those operations take time, are difficult to measure, and require sustained commitment. MISO is more than leaflet and loudspeakers—or in today's parlance more that tweets and Facebook posts. There is no magic tweet that will cause mass defections. The campaign must be well-planned, resourced, and sustained over time.

Warriors must heed the words of General Edward C. Meyer, former Army Chief of Staff who stated, "The keystone of our contribution toward peace is total competence in waging war. That expertise can only come from an ardent study of tactics and strategy."[49] Warriors must also recognize that the study of tactics and strategy must include the mind of the enemy as key terrain.

Notes

1. Secretary of State Hillary Clinton while speaking before the Senate Foreign Relations Committee on 2 March 2011, accessed 12 May 2018, https://www.dailysignal.com/2011/03/08/clinton-to-congress-we-are-losing-the-information-war/.

2. The Information Dominance branch was designated in April 2017. It includes cyber (17A), electronic warfare (EW) (FA29), and information operations (FA30) officers. As of October 2018, FA29 officers will be redesignated 17B. The EW field is being incorporated in the cyberspace operations career field.

3. Lieutenant Colonel Susan L. Gough, "The Evolution of Strategic Influence," (Carlisle Barracks, PA: US Army War College, 2003), 2.

4. Paul E. Valley and Michael A. Aquino, "From PSYOP to MindWar: The Psychology of Victory" (Headquarters, 7th Psychological Operations Group, United States Army Reserve, Presidio of San Francisco, 1980), 1.

5. In the words of Yogi Berra, "It's *déjà vu* all over again." Scott Stump, 'It's deja vu all over again': 27 of Yogi Berra's most memorable 'Yogi-isms', 23 September 2015, accessed 20 May 2018, https://www.today.com/news/its-deja-vu-all-over-again-27-yogi-berras-most-t45781.

6. Although propaganda has been in use since time immemorial, the US efforts in Vietnam were at an unprecedented scale given the ability to produce leaflets, and radio and television broadcasts. See Project CHECO (Contemporary Historical Examination of Current Operations), "Psychological Operations by USAF/VNAF in SVN," 16, and author's unpublished dissertation, "The Learning Curve: MACV's Grasp of Intelligence, PSYOP, and Their Coordination, 1965–1971," 15 May 2015, 41. Military information support operations (MISO) is the term now used by the Department of Defense instead of PSYOP.

7. For an excellent discussion of the development of PSYOP from WWII through Vietnam, see Lieutenant Colonel Susan L. Gough, "The Evolution of Strategic Influence," (Carlisle Barracks, PA: US Army War College, 2003.)

8. Michael G. Barger, "Psychological Operations Supporting Counterinsurgency: 4th Psyop Group in Vietnam," (Fort Belvoir, VA: Defense Technical Information Center, 2007), 8.

9. This seemingly small difference caused significant problems in the approach toward what intelligence was collected, processed, and disseminated. See Andrew Whiskeyman, "The Learning Curve: MACV's Grasp of Intelligence, PSYOP, and Their Coordination, 1965–1971," unpublished dissertation, 15 May 2015.

10. Military Assistance Command Vietnam, USMACV Directive 525-3, "Minimizing Non-Combatant Battle Casualties," 7 September 1965, Virtual Vietnam Archive, Texas Tech, accessed 13 October 2014, https://www.vietnam.ttu.edu/reports/images.php?img=/images/024/0240301028.pdf.

11. Military Assistance Command Vietnam, *Command History 1965*, Historical Research Branch, Office of the Secretary, Joint Staff; MACV, *Command History, United States Military Assistance Command Vietnam, 1965*, Headquarters Department of the Army, Information Management Support Agency, Alexandria, VA, 1966, 252.

12. General Westmoreland was not fixated solely on firepower as the solution to the problems in South Vietnam. The battle of Binh Gia in December 1964 had shown him the conventional threat. Directive 525-3 proved he had not forgotten about the unconventional one.

13. II Field Forces Vietnam, "Operational Report for Period Ending 31 October 1966," Headquarters II Field Force Vietnam, 15 November 1966, 12, 558.

14. Mervyn Edwin Roberts, *The Psychological War for Vietnam, 1960–1968* (Lawrence, KS: University Press of Kansas 2018) , 232.

15. Whiskeyman, "Learning Curve," 457.

16. *Hoi Chanh* was the Vietnamese term meaning "rallier" or "one whom returned to the righteous side" was the name given to those who rallied under the *Chieu Hoi* Program.

17. *Chieu Hoi* means "Open Arms" in Vietnamese. Military Assistance Command Vietnam, *Command History 1966*, 558.

18. Military Assistance Command Vietnam, *Command History 1965*, 452.

19. J.M. Carrier, and C.A.H. Thompson, *Viet Cong Motivation and Morale: The Special Case of Chieu Hoi* (Santa Monica, CA: RAND Corporation, 1966), v.

20. The plan developed included more US support, the construction of regional CHP centers in each corps, and changes to operational procedures. Additionally, six United States Agency for International Development (USAID) advisors and four US military liaisons would be assigned in support of the program, and by the end of 1965, three of the USAID advisors were on the job. The Government of Vietnam (GVN) agreed to construct a National *Chieu Hoi* center with scheduled completion in early 1966. A lack of qualified contraction bids delayed construction of the regional centers. Military Assistance Command Vietnam, "Command History 1965," 452.

21. Bob Considine, "Pacification cadres," *Philadelphia Inquirer*, 19 September 1967, cited in Frank L. Goldstein and Benjamin F. Findley, *Psychological Operations Principles and Case Studies* (Maxwell Air Force Base, AL: Air University Press, 1996), 100.

22. Bernard W. Rogers, *Cedar Falls-Junction City* (Washington, DC: US Government Printing Office, 1974), US Army Heritage and Education Center (AHEC) Collection.

23. Roberts, *The Psychological War for Vietnam*, 263 citing USIS Vietnam Feature Service, *Operation Cedar Falls . . . Out of the Iron Triangle*, 1, TTVA, DPC: Unit 2 – Military Operations, box 8, folder 7.

24. Rogers, *Cedar Falls-Junction City*, 19.

25. Roberts, *The Psychological War for Vietnam*, 263.

26. Rogers, *Cedar Falls-Junction City*, 56.

27. Typical of the leaflets was one written by Le Van Sa, in which he called out to his friends by name and gave them instructions on how to rally. Sa stated that he was being treated well and that he had been lied to by the VC. The leaflets written in Vietnamese (rather than being translated from English) were much more effective. Rogers, *Cedar Falls-Junction City*, 57.

28. Rogers, 57.

29. Roberts, *The Psychological War for Vietnam, 1960–1968*, 279.

30. Roberts, 396; see also Project CHECO, "Psychological Operations by USAF/VNAF in SVN," 14.

31. This conservative estimate did not include the additional one possible and one probable division-level units operating in the area. This brought the total enemy forces available to COSVN at the end of 1966 to nine division headquarters with personnel strength totaling 280,600. Military Region 5 was designated by the DRV and included the provinces south of the DMZ to Khanh Hoa and Darlac. See Ronald B. Frankum, Jr. *Historical Dictionary of Vietnam* (New York: Scarecrow Press, 2011), 291.

32. Joseph McChristian, *The Role of Military Intelligence* (Washington, DC: Department of the Army, 1974), 56.

33. Major G.S. Lorenz, et al., "Operation Junction City Vietnam Battle Book," Combat Studies Institute, 1983, 16.

34. Lorenz, 19–20.

35. COSVN was later referred to as the "Bamboo Pentagon" and was one of the factors that led President Richard Nixon to authorize the invasion of Cambodia. Some US military leaders were convinced that if COSVN HQ were destroyed, it would crush the North Vietnamese (NVN) efforts in the south, accessed 20 May 2018, https://www.atlasobscura.com/articles/the-myth-of-the-bamboo-pentagon-the-fabled-viet-cong-headquarters-that-pushed-america-into-cambodia. See also Lorenz, "Operation Junction City Vietnam Battle Book," 19–20.

36. Lorenz, "Operation Junction City Vietnam Battle Book," 16.

37. Rogers, *Cedar Falls-Junction City*, 135.

38. Rogers, 109.

39. McChristian, *The Role of Military Intelligence 1965–1967*, 55.

40. Rogers, Cedar Falls-Junction City, 151.

41. Rogers, 151.

42. William C. Westmoreland, *A Soldier Reports* (Garden City, NY: Doubleday, 1976), 282.

43. Evaluation of US Army Combat Operations in Vietnam (ARCOV), Volume 5, Annex, D-3-8.

44. Michael G. Barger, "Psychological Operations Supporting Counterinsurgency: 4th Psyop Group in Vietnam" (Fort Belvoir, VA: Defense Technical

Information Center, 2007), 1.

45. Terry F. Greene, "US Army Psychological Operations into the Year 2000," DTIC Document, 1993, 5.

46. 7th Psychological Operations Group. "Report on Psychological Operations Intelligence in Vietnam," Headquarters, 7th Psychological Operations Group, Target Analysis Section, 15th PSYOP Det (STRAT), 7th PSYOP Group, 17 November 1967, 10.

47. 7th Psychological Operations Group, "Report on Psychological Operations Intelligence in Vietnam," 1.

48. 6th PSYOP Battalion had two psychological operations interrogators who were supposed to have access to the interrogation facilities (according to DA PAM 33-1) but did not have official access to MACV J2 interrogation facilities. 7th Psychological Operations Group, "Report on Psychological Operations Intelligence in Vietnam," 2, 10.

49. Harry G. Summers, *On Strategy: A Critical Analysis of the Vietnam War* (New York: Presidio Press, 2009), 91.

Chapter 7
Gulf War—Infowar

Dorothy E. Denning
with Introduction and Notes by Robert M. Hill

2018 Introduction

In 1990 and 1991, the United States fought the Gulf War, a large-scale combat operation that pitted US and coalition forces against Iraq in order to liberate Kuwait from Iraq's annexation. Although the airland conflict (Desert Storm) was brief and, in hindsight, only moderately intense, the Gulf War was large-scale in that nearly 300,000 US Soldiers participated in the war, out of a total US force of more than one million—more than participated in either Korea or Vietnam at their peaks. Another feature of large-scale combat operations present during the Gulf War was the robust presence of echelons above brigade. The US contingent alone consisted of two Army corps, one Marine Expeditionary Force, seven Army divisions, and two Marine divisions.

The Gulf War was the first large-scale combat operation of the digital era, opening new possibilities to influence, deceive, manipulate, and shape not only the decision making of the enemy but of all relevant actors and audiences with a vested interest in the outcome of the conflict. Even if information warfare has existed since humankind's first conflict—largely in the form of deception—the revolution in new technologies from the 1960s on so dramatically changed the means and methods by which information could be used to "wage war" that it has taken almost three decades for the US military to fully embrace informational power as co-equal to physical power in the conduct of operations. The bottom line is that operations in any physical environment simultaneously occur in the information environment, the effects of which are less directly controlled but, as a result, must be carefully and deliberately planned.

In her seminal book, Information Warfare and Security*, Dr. Dorothy Denning, currently Emeritus Distinguished Professor at the Naval Postgraduate School, provides an introduction to information warfare just as the Dotcom bubble and other technological advancements were impacting every facet of business, politics, social interaction, education, as well as the nature of warfare.[*] In the first chapter, excerpted here, Denning explored the role information warfare played in the Gulf War, the history and nature of information warfare more broadly, and—from her 1998-vantage point—the trends she envisioned would play out in future years in terms of*

both technology and information warfare. Reading her work today, we see just how prescient she was.

For clarity's sake, Denning's use of information warfare is specific to her book and not intended to replace the currently approved doctrinal term information operations. As I am writing this introduction, there remains much discussion about the best term to define and describe operations, activities, and actions US forces undertake in the information environment to affect threat decision making, as well as influence a range of other audiences affected by military operations. Consensus seems to be emerging around the term operations in the information environment (OIE), cognizant of the fact that it is more encompassing of all that occurs in the information environment beyond simply a win-lose calculus against the threat or purely what IO forces and professionals do. For the purposes of this article, information warfare (IW) and information operations (IO) will be used interchangeably: IW is retained in Denning's text, while IO is used in my italicized 2018 notes, except in those select instances where IW aptly applies.

Before diving into Denning's first chapter, there are a few truisms about IO in large-scale combat operations to keep in mind that are summarized here and reflected in the notes that accompany Denning's text:

- ***Information is an element of combat power.*** *In 2017, the Chairman of the Joint Chiefs of Staff approved adding information as a joint function. The Army is presently considering whether to add information as a seventh warfighting function. Whether it is added or not, information is already an element of combat power but one often undervalued and underemployed. Perhaps initially, information was simply viewed as shared understanding. Shared understanding is critical to success but as an element of combat power, information is far more expansive and potent. Units and commanders who fail to integrate informational power with physical power will fail at consolidating gains achieved during large-scale combat operations, if not the combat operations themselves.*

- ***Information is ubiquitous and IO always active.*** *Tanks, maneuver forces, and artillery do not continuously move, shoot, or otherwise create effects in the operational environment; they do so only when an enemy is declared and authorization granted. IO, however, is always "on" or active; it does not rest or sleep.*

• ***Information is integral to all operations but IO varies by the capabilities available to execute it.*** *Because IO is always active, it supports any form or type of operation, across all levels and phases and the conflict continuum. IO execution, however, is not static or applied in boilerplate fashion. It is continually modulated to support other lines of operation or effort (or become itself the main operation or effort), optimizing available capabilities to create effects in the information environment necessary to seize, exploit, and retain the initiative therein.*

• ***There are limitations to IO that necessitate proactive and long lead time planning, speed, precision, creativity, and a strong defensive posture.*** *The United States will face enemies and adversaries that employ IO unconstrained by of the types of laws, policies, regulations, and ethical mores that govern its use by US forces. This merely means US forces must be far more proactive, innovate, nimble, and faster at applying lessons learned in the planning and execution of IO. They must also place extra emphasis on information protection to ensure unfettered decision making.*

• ***Every Soldier is an information warrior. One of the limitations of the terms IW and IO is that they tend to denote a function performed by specialized experts.*** *The sooner the Army trains every Soldier to be an information warrior the better. This begins with the simple realization that everything we do sends a message and we have a responsibility to align what we say with what we do so that our message is consistent with and reinforces the commander's intent, as well as higher headquarters' themes and narrative. This mindset extends to the fact that every Soldier is a sensor who must be able to report on indicators that show progress toward accomplishment of IO objectives. These basic skills are equally applicable to large-scale combat operations as they are to advise and assist or to counterinsurgency missions.*

The italicized notes that accompany Dr. Denning's text seek to complement, expand, and update her observations and conclusions with current and emerging Army thinking about operations in the information environment. Readers might opt initially to skip over the notes and read Denning's original text in its entirety. Doing so will provide a more contemporaneous account of the Gulf War from a pre-counterinsurgency (COIN) operations vantage point. They can then return to factor in the notes. The 2018 notes are in italics throughout this chapter.

Gulf War—Infowar

To illustrate the scope and diversity of information warfare even within a single area of conflict, this chapter begins with a brief account of information warfare incidents relating to the Persian Gulf War. It then summarizes a theory of information warfare and trends arising from new technologies.

The story starts with five hackers from the Netherlands who, between April 1990 and May 1991, penetrated computer systems at 34 American military sites on the Internet, including sites that were directly supporting Operation Desert Storm/Shield. They browsed through files and electronic mail, searching for keywords such as nuclear, weapons, missile, Desert Shield, and Desert Storm. They obtained information about the exact locations of US troops, the types of weapons they had, the capabilities of the Patriot missile, and the movement of American warships in the Gulf region. When they were done, they removed traces of their activity from system logs to conceal their hacking spree.[1]

Large-scale combat operations do not simply pit one nation or actor against another; they involve multiple entities—state, nonstate, criminal, and terrorist—each vying to ensure their vested interests predominate, are advanced or, at the very least, are protected and preserved.

According to Jim Christy, program manager of computer crime investigations and information warfare at the Air Force Office of Special Investigations, the targets included military supply systems. "They didn't, but they could have, instead of sending bullets to the Gulf, they could have sent toothbrushes," he said.[2] Eugene Schultz, then manager of the Department of Energy's Computer Incident Advisory Capability, said that the hackers had so much information that they filled up the disks on the machines they used to launch the attacks. They also filled several floppy disks. When they ran out of places to store their loot, they broke into computers at Bowling Green University and the University of Chicago and downloaded the information, figuring they could transfer it somewhere else later.[3] By some accounts, the Dutch hackers tried to sell their pilfered information to Iraq during the Gulf conflict. Schultz said he told the British Broadcasting Corporation that he had been informed through government officials that Saddam Hussein had been offered the data through an intermediary working on behalf of the hackers. Schultz also reported that Baghdad, fearing a trap, declined the offer.[4]

As the example of the Dutch hackers reveals, the United States may have to "fight" an array of third-party entities—whose objective is merely

to prove their moxie, make money or mischief, or have fun—simultaneously with a declared enemy. IO must be planned and executed—across the whole of government—to consider all relevant threats, actors, and audiences.

Even though the hackers were identified, the United States was powerless to do anything about it, Schultz said. At the time, computer break-ins were not illegal in the Netherlands. The Federal Bureau of Investigation almost lured the lead attacker to the United States under the guise of an interview with a major aerospace firm in Florida, but the hacker inadvertently was tipped off. Two of the five eventually ended up in jail, but not for the US military intrusions. They were convicted of credit card fraud.[5] Meanwhile, Baghdad had access to inside spies. In May 1991, Juergen Mohhammed Gietler, a 42-year-old archivist for the German Foreign Ministry, was sentenced to five years in prison for passing Western military and political intelligence to Saddam Hussein on the eve of the Gulf War.

Threat espionage and many forms of sabotage are elements of IW as these acts seek to gain an information advantage over the United States. We must assume that anything and everything about us (i.e., the United States and its partners) can and will be used against us. Not only will the truth be weaponized against us but also the untruth.

Gietler gave Iraqi agents in Bonn hundreds of documents before his arrest, including letters between President George Bush and Chancellor Helmut Kohl about US military plans to move troops and weapons through Germany, reports describing what Western intelligence agencies knew about foreign companies helping Iraq build weapons of mass destruction, confidential estimates on Iraq from the US State Department and from NATO, German intelligence reports on Iraq's missiles and maps showing where they were located and likely targets in Israel, French satellite images showing Israeli missile sites, and a list of how many US stealth bombers were being deployed to the Gulf region. In reaching its guilty verdict, the Dusseldorf court ruled that the meaningful military intelligence brought Iraq "considerable advantages."[6] After serving his five-year sentence, Gietler said on a CBS *60 Minutes* segment that providing allied secrets to Iraq was "permanent fun, five days a week." He said he was paid for his spying but that money was not his motive. "I was on the Iraqi side," he told the news magazine. "I felt it was my duty." He said that after meeting Iraq's military attaché, General Osmat Joudi Mohammad, by chance at a restaurant, he volunteered to supply the information. Gietler was arrested after German counterintelligence agents intercepted a phone call by Osmat.[7]

The United States and its allies had their own sources of intelligence, including satellites, unmanned aerial vehicles (UAVs), and Iraqi defectors. In 1990, US spy satellites saw Iraqi forces massing on the Kuwaiti border, although an invasion was discounted after Arab allies said Saddam Hussein was bluffing.[8] Also before the war broke out, satellite imaging systems mapped potential target areas. The maps were put on board Tomahawk cruise missiles during the war and compared with images taken by the missiles' own radar.[9] The Global Positioning System (GPS), a 24-satellite constellation that emits signals used for determining location, helped coalition land forces navigate the desert terrain. GPS was used by aircraft to map minefields accurately and by US warships to obtain correct launch positions for missiles.[10] UAVs orbited the battlefield, using video and infrared imagery to provide real-time tactical information on the movements of Iraqi troops and bomb damage assessment. These drone aircraft logged a total of 530 missions and 1,700 hours of flight time. Iraqi troops even surrendered to one.[11]

Gaining and maintaining contact with the adversary is necessary to reveal the adversary's areas of influence and dispositions; therefore, intelligence support to IO is essential to exposing the adversary's intent in the information environment. Technology increasingly offers a more diverse array of intelligence-gathering platforms, but more information does not necessarily mean better intelligence, particularly when it comes to discerning the threat's "mind" and modes of decision making.

Equally important, coalition forces neutralized or destroyed key Iraqi information systems with electronic and physical weapons. During the first moments of Operation Desert Storm, clouds of antiradiation weapons fired from helicopters and aircraft disabled the Iraqi air defense network. Ribbons of carbon fibers, dispensed from Tomahawk missiles over Iraqi electrical power switching systems, caused short circuits, temporary disruptions, and massive shutdowns in power systems.[12] An Air Force F-117 Stealth fighter directed a precision-guided bomb straight down the air-conditioning shaft of the Iraqi telephone system in downtown Bagdad, taking out the entire underground coaxial cable system, which tied the Iraqi high command to their subordinate elements. This eliminated the primary method of communications between the command center in Bagdad and subordinates in the field.[13] Once the command and control centers were out of action, the coalition went after Iraq's radar systems, taking away their ability to "see" the battlespace.[14] Blind and deaf, Iraq had little chance of victory.

IO is lethal and nonlethal but never strictly offensive or defensive; it modulates among attack, defend, and stabilize weighted efforts in support of lines of operation or lines of effort. In other words, IO's focus is not so much the type of operation but the type of effects that need to be generated in and through the information environment to support the large-scale operation being undertaken.

According to one tale, the allies further disabled Iraqi military computer systems with a computer virus, shipped to Iraq in printers. The story, which aired January 10, 1992 on ABC's *Nightline* following publication in *US News & World Report*, said the US government targeted the virus at Iraqi's air defense. A few weeks before Operation Desert Storm, a virus-laden computer chip allegedly was installed in a dot matrix printer that was assembled in France and shipped to Iraq via Amman, Jordan. The virus was said to have been developed by the National Security Agency (NSA) and installed by the Central Intelligence Agency (CIA). It apparently disabled Windows and mainframe computers. The operation was said to have worked.

Cyberspace is a domain that is fully a part of the information environment. To achieve synergy, IO and cyberspace electromagnetic activities (CEMA) are closely coordinated. As Gantz's story reveals, most cyberspace effects are planned and executed at the operational and strategic levels, but tactical units can request cyberspace operations and electronic warfare support, through channels, using standard message formats (see FM 6-99).

The story originated from John Gantz's weekly *Infoworld* column on 1 April 1991. Gantz had reported that the NSA had written a computer virus dubbed "AF/91" that would "attack the software in printer and display controllers." The column went on to say that "By January 8, 1991, Allies had confirmation that half the displays and printers . . . were out of commission." It concluded with: "And now for the final secret. The meaning of the AF/91 designation: 91 is the Julian date for April Fool's Day." As Winn Schwartau observed, AF/91 also denotes April Fool's, 1991. According to a letter from Gantz to Schwartau, *Infoworld Japan* picked up the story and translated it to Japanese, in the process losing the meaning of "April Fool's." *US News* had gotten the article from their Tokyo Bureau, which in turn had gotten it from the *Infoworld Japan* piece.[15] What began as a practical joke had become national news. It was a hoax.

During the Gulf War, both sides exploited television to their advantage to influence perceptions and public opinion. Shortly after invading

Kuwait, Saddam's "EliteRepublicanGuards" (spoken as one word by TV journalists) faked a retreat in front of the cameras of global television. In fact, Iraq was reinforcing its grip on the country.

Reports from CNN's Peter Arnett in Bagdad were skewed by the limited amount of satellite time he had available to coordinate his reportage, as well as the best efforts of his Iraqi minders, who were bent on using CNN as an instrument of propaganda. Even prior to his arrival, the Iraqi censors scored big when CNN aired, live as received, Iraqi-provided video. Saddam's propagandists also gained direct access to the friendly Jordanian television system, causing anti-US and anti-Alliance riots in Jordan.[16] Some Iraqi propaganda backfired. When Saddam boasted that Iraq would win because they were prepared to sacrifice thousands of soldiers whereas the Americans could not stand the loss of even hundreds, his troops realized he was talking about sacrificing them. This was said to have contributed to their willingness to defect and surrender.[17]

Deception is fundamental to large-scale combat operations. It's not a skill reserved only for the IO or military deception officer or designated representative. MILDEC is a competency that every unit and individual must possess, to varying degrees.

US forces staged several amphibious exercises along the Saudi coast in front of CNN crews in order to trick Saddam into believing that the coalition planned an amphibious assault to flank Iraqi forces along the Kuwaiti border. The deception paid off, as several Iraqi divisions were tied down defending the coast from an allied Gulf landing.[18]

As the example of the amphibious exercises demonstrates, the most effective deceptions are rooted in truth.

One news story depicted Iraqi soldiers yanking Kuwaiti babies out of incubators. The story apparently was hyped by an American public relations firm hired by a Kuwaiti government-backed organization. The only eyewitness to the horror was the 15-year-old daughter of the Kuwaiti ambassador to the United States. After investigating, ABC's *20/20* reporter John Martin found little proof that the story was anything more than propaganda. At the time, however, the story had a major impact on policy makers in the United States. President Bush is said to have mentioned the "incubator atrocities" eight times in 44 days, and seven senators brought it up during debate over the war. The war resolution passed by only five votes.[19]

The amount of "fake news" on all sides is increasing at an exponential rate. Its intentional use by US forces—particularly if its aim is to influence

audiences other than the enemy or an adversary—is problematic and runs the risk of being illegal, immoral, or both.

During the war, the allies dropped 29 million leaflets behind Iraqi lines. The leaflets, which came in 14 varieties, reached approximately 98 percent of the 300,000 troops. They were tested on cooperative prisoners of war, whose recommendations included removing any trace of the color red (a danger signal to Iraqis), showing allied soldiers with beards (convey trust and brotherhood in Iraqi culture), and add bananas (a great delicacy) to a bowl of fruit shown being offered to surrendering Iraqis. The Voice of the Gulf was broadcast over six clandestine radio stations, including both air and ground stations. During its period of operation in early 1991, a total of 189 psyop (psychological operations) messages were aired. Additional messages were broadcast from loudspeakers in manpacks, vehicles, and helicopters during ground campaigns.[20]

Military information support operations (MISO) provide a wide array of means to reach the enemy or adversary, such as printed products, radio, and loudspeakers. MISO programs must be approved through channels, typically requiring a long lead time to plan properly.

The leaflets and broadcasts conveyed the inevitability of Iraq's defeat. Over 40 percent of the leaflets were appeals for surrender; seven percent urged Iraqi troops to abandon their weapons and flee. The messages, which were part of the campaign in psyop and perception management, attempted to reassure Iraqi soldiers that they would be treated well in allied hands. They blamed an "evil" Saddam for the war, depicting the solders as brave men who had been led astray. The messages stressed Arab brotherhood and peace or warned that Iraqi commanders would be held accountable for war crimes against Kuwaiti people and property. To deter use of chemical weapons, messages warned that Iraqi soldiers were ill equipped with protective gear and that commanders would be punished.[21]

MISO products (and the scheme of IO more broadly) require an acute understanding of the full range of target audiences in the area of operations, including the enemy. PSYOP forces bring the ability to conduct target audience analysis, which is essential to crafting the right messages and ensuring their delivery at the right time and place in order to achieve psychological objectives in support of the commander's intent.

According to the American Red Cross, nearly 87,000 Iraqi soldiers turned themselves over to coalition forces, most of them clutching the leaflets or hiding them in their clothing.[22] A postwar survey of 250 prisoners of war found that 98 percent had seen the leaflets, 58 percent heard

radio broadcasts, and 34 percent heard loudspeaker broadcasts. The soldiers found the messages credible, with 88 percent saying they believed the leaflets, 46 percent the radio broadcasts, and 18 percent the loudspeaker broadcasts. The POWs also reported that their decisions to surrender or defect were influenced by the messages, with 70 percent saying they were influenced by leaflets, 34 percent by radio broadcasts, and 16 percent by loudspeaker broadcasts.[23] A captured general said that "Second to the allied bombing campaign, PSYOP leaflets were the highest threat to the morale of the troops."[24]

The Red Cross statistics cited here also demonstrate the necessity of conveying messages via multiple platforms. Repeated messages from multiple sources are more likely to "stick."

Iraq's own program in psyop was much less successful, failing in part because they did not understand American culture. For example, they used a woman, "Baghdad Betty," to make broadcasts aimed at disillusioning American soldiers. She lost credibility early on, however, when she told the soldiers that their wives and girlfriends back home would be sleeping with Tom Cruise, Tom Selleck, and Bart Simpson. It was ridiculous enough suggesting that the women would be seduced by movie stars, but a cartoon character?[25]

At the end of the war, Soviet General S. Bogdanov, chief of the General Staff Center for Operational and Strategic Studies, said: "Iraq lost the war before it even began. This was a war of intelligence, electronic warfare, command and control and counter intelligence. Iraqi troops were blinded and deafened. . . . Modern war can be won by informatika and that is now vital."[26] Psyop and perception management also played an important role, not only with Iraqi soldiers but also with the public. When Kuwait City was liberated, images on television showed hundreds of Kuwaitis waving American flags as liberating forces entered the city, demonstrating their support for American efforts. A public relations firm had earlier arranged the mass distribution of the handheld American flags, as well as lapel pins.[27]

As the quote from General Bogdanov makes clear, adversary military commanders consider IW not simply as another element of their combat power but one that is decisive. In 2017, the US Department of Defense designated Information as a joint function in recognition of its parity with other functions in achieving military and national objectives.

After the Gulf War, the United States, through the CIA, reportedly continued to use perception management in an attempt to overthrow Sadd-

am Hussein. The operation, eventually broken apart by the Iraqi president, used radio broadcasts and other media for spreading messages. In a 1997 interview, Warren Marik, retired CIA agent, said a Washington-based public relations firm produced radio scripts and videotapes denouncing the regime. The scripts, which called on Iraqi army officers to defect, were broadcast on two large radio transmitters the CIA established and managed in Jeddah, Saudi Arabia; and Kuwait. Additional stations sprang up in Cairo and Amman. Marik also reported that unmanned aircraft dropped leaflets over Baghdad ridiculing the Iraqi dictator on his birthday.[28]

IO and the various capabilities it synchronizes are involved in perception management; that is, they seek to affect the way that various audiences perceive or construct their reality so it is favorable to US and allied objectives. As this article suggests, the term perception management is typically applied to non-military efforts that must be part of a whole-of-government approach to operations in the information environment.

The challenge with perception management that confronts the United States and many of its allies is the rules by which it is employed. Enemies and adversaries are quite willing to do whatever is necessary to get the United States and its Unified Action Partners to believe what they want us to believe, with little or no concern for the truth. Legally and morally, US forces must be able to articulate clearly—and then enforce—the allowable limits of shaping, shading, or disregarding the truth in pursuit of military objectives.

Iraq has continued its intelligence activities. In November 1997, US military and intelligence officials reported that Iraqi intelligence agents successfully spied on United Nations weapons inspectors in 1996 and 1997. The methods used included eavesdropping, wiretapping, and placing spies in the U.N. camp. Secretary of Defense William Cohen said in a television interview that "the Iraqis have always watched every move the inspectors have tried to make. They anticipate where they're going. They may have, in fact, penetrated their inspection team." Officials said the team might even be under surveillance at U.N. headquarters in New York.[29]

Iraq's agency for electronic eavesdropping, known as Project 859, is staffed by almost 1,000 technicians and analysts who monitor satellite telephone calls and other telecommunications from six listening posts in the country. International calls are picked up at a switching post in Al Rashedia, where Project 859 headquarters are located. There, messages are taped and analyzed by Iraqi intelligence officers. The agency may have the ability to decode some scrambled calls.[30]

The nation's largest intelligence agency is the Iraqi Intelligence Service, which is responsible for spying overseas. It is believed to have members working abroad under diplomatic cover. The two agencies report to the Special Security Organization, which collects information about all threats, domestic and foreign, to Saddam.[31] On 19 October 1997, Israel's general security service, Shabak, arrested two people suspected of spying for Iraqi military intelligence. One of the persons, 37-year-old Yukhar Faran, had emigrated to Israel with false papers identifying him as the son of a Jewish family that remained in Iraq. The second person, 30-year-old Joseph Hirsch, also held Israeli citizenship. Both operated out of the port of Ashdod.[32]

American "eyes and ears" watch over Iraq to ensure Iraqi compliance with agreements on weapons inspections. The airborne surveillance system has three layers: Keyhole KH11 photographic reconnaissance satellites orbiting at an altitude of about 660 miles, US Air Force U2R spy planes operating from up to 90,000 feet, and US Navy ES3A "Shadow" Viking aircraft, which can pick up military radio signals from 34,000 feet.[33] In June 1998, Richard Butler, the Australian diplomat who heads the U.N. Special Commission (UNSCOM) charged with eliminating Iraq's weapons of mass destruction, showed photographs suggesting that Iraq had buried some missile parts and then dug them up again after inspections. The photos, which were backed up by satellite images, were presented as evidence that Iraq was still hiding illegal weapons.[34]

Iraq allegedly used deception to cover up its weapons programs. During the three-week interruption of U.N. searches for hidden weapons in late 1997, Iraq apparently moved equipment that could be used to produce forbidden missiles out of range of U.N. surveillance cameras. Butler said the equipment included "gyroscope rotor balancing equipment which could be used to balance prohibited missile gyroscopes." He also said that it appeared the Iraqis had tampered with U.N. cameras, covered lenses, and turned off lighting in facilities under monitoring.[35] Information underpinning the entire Iraqi nuclear, biological, and chemical warfare program was said to be stored on computer hard drives and disks that were constantly moved from one location to another in an effort to frustrate the U.N. team.[36]

Iraq has also continued its use of psyop and perception management. When U.N. inspectors resumed their business after the crisis that had barred Americans from the inspection team, thousands of Iraqis shouted "Down with America" as they took part in a mass funeral for dozens of

children. Iraq blamed the deaths on U.N. sanctions, claiming the children had died from lack of food and medicine.[37]

Perception management can be viewed as the means by which the Information instrument of national power is exercised. It is also increasingly becoming the chief instrument by which state, non-state, terrorist, and criminal actors achieve their aims. Of the four instruments (DIME: diplomatic, information, military, economic), information is the one that is in continual use. Therefore, it must be planned and executed continually across the cooperation-competition-conflict continuum. There is no pause or break in action with information. Like Iraq during the post-Desert Storm period, adversaries will not hesitate to do everything they can to shape our perceptions favorable to their ends. US forces must do likewise, both to counter threat narratives and promote their own such that they decrease the need for large-scale combat operations and enhance their success should they become necessary.

Later, Iraq accused the United States of planning air strikes to plant fake chemical or germ warfare evidence at "presidential sites" declared out of bounds to U.N. inspectors.[38] Butler and others, for their part, voiced suspicions that these mammoth complexes, some of which stretched for several miles, were being used to hide weapons of mass destruction from the inspectors. The Clinton administration estimated there were 78 of these presidential sites.[39] One covered 31.5 square miles and contained 1,058 buildings.[40]

When the crisis over U.N. inspections and the threat of an American air strike ended in early 1998, Iraq portrayed Saddam as the winner. Television broadcasts showed a beaming Saddam waving an old rifle as he visited village after village. Adoring crowds were dancing, singing, and clapping as Saddam waved from a balcony.[41]

Information Warfare

The brief history of the Gulf conflict presented here illustrates several types of information warfare operations—computer intrusions, human spies, spy satellites, eavesdropping, surveillance cameras, electronic warfare, physical destruction of communications facilities, falsification of papers, perception management, psychological operations, and computer virus hoaxes. There are others—theft of trade secrets, privacy invasions, and e-mail forgeries, to name a few. Depending on the circumstances, some acts are crimes. Others are unethical even if legal. Still others are considered acceptable practices, of governments if not other parties. Some operations are affiliated with military conflicts. Others are situated in broader

conflicts at an individual, organizational, or societal level. What they have in common is that they all target or exploit information resources to the advantage of the perpetrator and disadvantage of another.

Information has always been a component of warfare but its impact has become more acute given technological advancements and the pervasiveness and instantaneousness of information across all aspects of life. Although Army doctrine has addressed information as a component of operations for decades, it wasn't until the mid-1990s that it achieved parity with other elements of combat power and warranted its own field manual. In the intervening 25 years, IO has gone through three name changes (information environment, inform and influence activities and back to information operations). As of the publication of this desk reference, it is uncertain whether IO will again be rebranded as information warfare (IW), operations in the information environment (OIE), or another term yet to be decided. The bottom line is this: as an element of combat power, information has often been misunderstood, under-valued, and under-utilized. Whatever term is applied, commanders and units must be adept at optimizing this element of combat power in concert with all other elements.

In the preface to Winn Schwartau's book *Information Warfare*, John Alger, then dean of the School of Information Warfare and Strategy at National Defense University, wrote, "Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary."[42] A December 1996 directive from the Office of the Secretary of Defense defines information warfare as "Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries," where information operations are "Actions taken to affect adversary information and information systems while defending one's own information and information systems."[43]

This book [Denning's *Information and Security*] attempts to take these definitions deeper, to provide a theory of information warfare based on the value of information resources to an offense and defense. An offensive operation aims to increase the value of a target resource to the offense while decreasing its value to the defense. A defensive operation seeks to counter the potential loss of value. Information warfare is a "win-lose" activity. It is about "warfare" in the most general sense of conflict, encompassing certain types of crime as well as military operations.

The value gained by the offense can have a monetary component, as when intellectual property is stolen and sold, but this is not always the case. In destroying and disrupting Iraqi command and control and radar systems during the Gulf War, the United States and its allies gained a military advantage over Iraq. Disabled, the systems became virtually useless to Iraq but of great strategic value to the allies, who took advantage of Saddam's blindness and inability to communicate with his troops. It would be impossible to assign a dollar value to these systems, before or after the attack, to either side. Similarly, it would be difficult to assign a dollar value to the advantage gained by Saddam in censoring the broadcasts of his adversaries.

As currently defined, IO is about affecting enemy or adversary decision making while protecting our own. Decision making cannot occur without information or, using Denning's lexicon, without information resources, whether these resources are physical (cell tower, computer hardware), informational (algorithms, software, data processing), or human/cognitive (perception, biases, sense making).

The value of an information resource to a player is a function of six factors. First is whether the resource is relevant to the concerns and commitments of the player. Second is the capabilities of the player. The player must have the knowledge, skills, and tools to use the resource effectively. Third is the availability of the resource to the player, and fourth is its availability to other players. Often, a resource has the most value to a particular player when it is readily available to that player but not to others. When Gietler sold Western intelligence documents to Iraq, for example, their value to the allies was diminished. Iraq, on the other hand, gained from the acquisition. Fifth is the integrity of the resource, which includes completeness, correctness, authenticity, and overall quality or goodness. In general, the greater the integrity, the more reliable and hence valuable a resource to particular player—unless it is the player who intentionally corrupts the resource. Then lack of integrity can be used to advantage. This happened when the allies staged the amphibious exercises in front of CNN cameras, compromising the integrity of Iraq's source of news and giving the allies an advantage in their ground-based attacks. The sixth and final factor is time. The value of an information resource can increase or decrease with time.

Offensive information warfare operations produce a win-lose outcome by altering the availability and integrity of information resources to the benefit of the offense and to the detriment of the defense. In so doing, they

may also alter the concerns, commitments, and capabilities of the defense, but the immediate effect is a change of availability or integrity. There are three general outcomes. First, the offense acquires greater access to the information resource; that is, the availability of the information resource to the offense is increased. This was illustrated by the Iraqi acquisition of intelligence documents from the German spy and the allied acquisition of information about the battlespace from spy satellites. Second, the defense loses all or partial access to the resource; that is, the resource becomes less available to the defense. This was illustrated by the attacks that sabotaged Iraq's command and control and radar systems and by Saddam's censoring of broadcast media. Third, the integrity of the resource is diminished. This was illustrated by the TV broadcasts that aired misleading or distorted stories such as the amphibious exercises. Many operations produce multiple effects. Acts of sabotage, such as those against Iraq's command and control systems, both deny access and damage integrity. Computer intrusions give the hacker greater access to computer systems while diminishing the integrity of the systems, especially if files are altered. Some operations begin with an acquisition phase, then move on to sabotage, or use a combination of both throughout.

Offensive information warfare is a win-lose activity. It is usually conducted without the consent of the defense and often without their knowledge. Even when the defense apparently agrees to participate, it is without fully understanding the motives of the offense and the consequences to themselves. The insider who reveals a password to a hacker on the other end of a phone call who says it is needed to fix a problem does not know the hacker's true intent.

Denning uses "win-lose" to refer to the intended result of a single operation, not a whole campaign or sustained effort. It is adversarial as opposed to "win-win". To win, one side or the other must gain a window of advantage in the information environment and hold the advantage long enough that the other side makes a fatally-flawed decision or believes it cannot prevail.

As the Gulf War example illustrates, information warfare involves more than destructive acts. Many acts of acquisition, such as covert intelligence operations, aim to leave originals intact. The objective is to get the information without being detected. Media manipulation and censorship are also nondestructive acts, aimed at influencing perceptions and beliefs.

IO involves risk. When units employ it against the threat, they must be cognizant of second and third order effects—of both intended and un-

intended consequences. They must also recognize that destroying threat information resources might achieve a temporary, tactical advantage that is offset by a longer-term disadvantage. Defensively, it is impossible to achieve an impenetrable shield against enemy IW efforts. There will always be gaps or vulnerabilities that can be exploited. Commanders must weigh the costs of achieving ever-higher levels of security with the benefits, which may offer diminishing returns.

Defensive information warfare seeks to protect information resources from attack. The goal is to preserve the value of the resources or, in the event of a successful attack, recover lost value. Defenses fall in six general areas: prevention, deterrence, indications and warnings, detection, emergency preparedness, and response, although specific operations and technologies may fall in more than one area.

In IO's definition, the phrase "while protecting our own" is almost an after-thought. It is anything but secondary. Given the legal and moral limitations and/or prohibitions placed on US forces that delimit offensive—or attack-weighted IO efforts, protecting friendly information may be the primary means by which US and allied forces gain advantage in the information environment.

Defensive information warfare is closely related to information security. They are not, however, identical. Information security is concerned mainly with owned resources and with protecting against errors, accidents, and natural disasters as well as intentional acts. Defensive information warfare addresses non-owned resources, including broadcast and print media in the public domain, but is not concerned with unintentional acts. The term "information assurance" is often used to encompass both information security and defensive information warfare.

Information warfare involves much more than computers and computer networks. It encompasses information in any form and transmitted over any media, from people and their physical environments to print to the telephone to radio and TV to computers and computer networks. It covers operations against information content and operations against supporting systems, including hardware and software and human practices.

Offensive information warfare operations succeed by exploiting vulnerabilities in information resources. These vulnerabilities can arise in hardware and software components and in human practices. They can be introduced at the time products are developed, delivered, installed, configured, used, modified, and maintained. Implementing airtight defenses is extremely difficult, and security holes are discovered in areas where they

were not expected. Although many information resources can be reasonably hardened against all but the most sophisticated outsider attacks, 100 percent security is neither possible nor worth the price. Computer systems are tremendously complex, containing millions of lines of code. No single person can comprehend that much code well enough to confirm that it is free of security holes or hidden trapdoors. Moreover, systems and environments change, and even the most thoroughly studied and highly protected resources are generally vulnerable to threats from insiders with access. The goal is risk management, not risk avoidance at all cost.

Vulnerabilities in themselves do not constitute a threat to information resources. Nor does the existence of methodologies to exploit those vulnerabilities. A threat arises only when there is an actor with the intent, capability, and opportunity to carry out an attack. Defensive information warfare aims primarily to protect against credible threats, especially those that have some reasonable chance of occurring and could lead to substantial losses. A goal of this book is to make some assessment of what those threats and losses are today and what they are likely to become in the future. Toward that end, emphasis is on actual incidents that have taken place and on observable trends.

From Chicks to Chips

This section is substantially edited for length. See Denning's book for the complete version.

Information warfare is not new. It is not a "third-wave" phenomenon nor a by-product of the computer revolution. Indeed, it is not even unique to the human species. Take the cuckoo bird. This information warrior has duped as many as 180 different species into foster parenthood by laying its eggs in the nests of other birds. To avoid detection, it adjusts the egg's morphology to that of the host. Through its behavior, it destroys the integrity of the information environment of its host. The visual appearance of an egg is no longer a reliable source of information.[44] As another example, the raven makes phony submissive gestures to hated rivals in order to entice them to come close. When they do, it makes an abusive attack. Again, it has compromised the integrity of its adversary's information environment.[45] Plants and animals also employ methods of defensive information warfare to guard information that is crucial to their survival. For example, they may be countershaded or have special coloration in order to make them inconspicuous to species that are higher up on the food chain.

Denning uses an apt phrase when discussing the raven's use of IO/IW: compromising the integrity of the adversary's information environ-

ment. Put another way, the information environment is everything in our surroundings that enables us to make sense of things, formulate thoughts, make decisions, and take action. IO is about affecting the information environment so that it confounds the enemy's ability to do these things while preserving our own ability to make swift, accurate, and fully informed decisions. Although IO tends to focus routinely on synchronizing information-related capabilities to achieve these ends, in large-scale combat operations, any and all capabilities must be harnessed to create effects in the information environment that optimize the information element of combat power or informational power.

Human beings have always been concerned with protecting prized information from adversaries. Some 5,000 years ago, Chinese emperors guarded the secret of silk production—the larval worm that produced the fiber, the mulberry plant that provided its food source and place of dwelling, and the weaving techniques that transformed the fibers into elegant cloth—with the threat of death by torture. Their security system worked for about 3,000 years, when the secret was carried out by a princess who left to marry a prince in a far-off land.[46] In 1500 BC, a Mesopotamian scribe guarded the secret to pottery glazes with a less threatening method. He encoded the recipe in cuneiform signs on a clay tablet.[47] In the first century BC, Julius Caesar, fearing his messages would be intercepted, wrote to Cicero and other friends in a secret code that today bears his name.[48]

Even though information warfare is not new, it has been transformed by new information media and technologies. At the turn of the twentieth century, an information warrior would not have contemplated hacking into a computer system to steal secrets, launching a destructive computer virus onto a network, intercepting cellular phone calls, gathering imagery with spy satellites, or broadcasting propaganda and disinformation over radio and television stations. The technologies simply did not exist. By 1950, computers had been invented (as well as radio and TV), but hardly anyone had them and none of them were connected or even remotely accessible. There were no Web sites to hack, no Internet service providers to take down, no Web transactions to intercept, and no e-mail for delivering malicious code. There was no low-cost method whereby an ordinary person could reach potentially millions of people with destructive computer viruses, hate messages, hoaxes, and conspiracy theories.

It was not until the 1960s that computers began to be interconnected, initially on local area networks within an organization. By 1969, the first wide area network was operating in the United States. Named after its sponsor, the Department of Defense Advanced Research Project Agency,

ARPANET connected Stanford Research Institute, the University of California at Los Angeles, the University of California at Santa Barbara, and the University of Utah. It eventually evolved into the Internet—a network of networks that spans the globe.[49] When ARPANET was finally decommissioned in 1990, there were more than 300,000 hosts on the Internet. This jumped to 1 million in 1992, 10 million in 1996, and 30 million by 1998. As of September 1998, the Irish firm NUA Ltd. estimated that 147 million people worldwide were using the Internet.[50]

We approach the end of the [20th] century with computers everywhere. They are cheap, often tiny, frequently interconnected, and incorporated into everything from microwave ovens to precision guided missiles. They have been integrated into all types of processes, including business processes, banking and finance, transportation and navigation, energy and water delivery, education, entertainment, government, health care, emergency services, and military operations. They have enabled electronic commerce, telemedicine, teleconferencing, and telecommuting. A consequence is that sensitive information, once confined to conversations and paper documents in offices, is now computerized and transmitted over public networks—making it potentially vulnerable to theft, exploitation, and sabotage by distant parties.

Advances in computing have been joined by equal advances in sensors. They too are cheap, tiny, pervasive, and connected to other technologies. They are paving the way to a future when information in the environment is readily available to remote persons. Already, some day care centers let parents watch their children while browsing the Web. Video cameras are placed in the rooms where the youngsters play and then fed to the center's Web site.[51] Although access to the sites is restricted to parents, are there risks to the children if the sites are hacked? Will totalitarian governments install such systems everywhere so they can watch their citizens? Andrew Leonard, technology correspondent for Salon, observed: "Just imagine how tempting that kind of Net-enabled Panopticon will be in a country whose leaders have always looked upon the [population] as one big mass of pre-schoolers."[52]

While new technologies have enabled new methods of information warfare, old methods have persisted and are likely to continue to do so. Spies still penetrate organizations to steal their secrets and police use undercover operations to infiltrate organized crime groups. Military units use visual surveillance along with high-tech sensors and other gadgetry to acquire information about the battlespace. They engage in deceptive maneuvers to fool the enemy and in psyop and perception management to

influence behavior. They use bombs and other physical weapons to take out enemy communications systems.

Perception management in particular is likely to play a significant role in future operations. John Petersen predicts that information warfare in the future will look much like advertising, convincing people to behave in ways that meet the objectives of the warrior. Information warfare will move away from hardware toward ideas and perceptions. It will involve the manipulation of "memes"—big, powerful ideas such as global warming and nuclear war that move people to action and the manipulation of perceptions through such means as holographic projections.[53] Human history has been shaped by memes, religion being a good example, so Petersen's projection might be viewed as a continuation of age-old methods.

Our adversaries, Russia in particular, have become masters of perception management, largely through the use of misinformation and disinformation. An excellent primer on their techniques and ways to counter them is found in Christopher Paul's and Miriam Matthews' publication The Russian "Firehose of Falsehood" Propaganda Model*, available online through the RAND Corporation.*[54]

The big question is this: Can someone launch an attack with catastrophic consequences and, if so, what are the chances of that happening? In truth, nobody knows. It is easy to postulate scenarios such as "Stock market crashes after hacker tampers with Wall Street computers" or "Planes collide after terrorists hack into navigation system and alter routes." It is much more difficult to assess whether a scenario is plausible or likely. Several factors must be considered, including vulnerabilities in technologies and the way they are used, the capabilities needed to exploit those vulnerabilities, redundancies and other safeguards that compensate for weaknesses, and whether there are people with the capabilities, motive, and opportunity to carry out an attack.

Denning raises the specter that IW will involve more than purely military means to achieve an adversary's aims. Simultaneous to physical attacks in distant areas of operations, the threat will employ informational attacks on the homeland, such as against power grids, information networks, telecommunications infrastructure, banking, and so on. There will also be psychological attacks across all media platforms designed to spread propaganda, disinformation, and misinformation, as well as sow uncertainty and discord. This future reality demands a robust whole-of-government approach to information, as well as mutual, reinforcing support from Unified Action Partners. Due to its size and budget,

the Department of Defense will play an outsized role in coordinating this whole-of-government approach to the threat's use of IW and our response to it. The increasing level of connectedness among systems—both governmental and nongovernmental—means that attacks to any part of the system threatens all others and national security.

What we do know is that information systems are vulnerable and there are people who are motivated to do bad things. For this reason, it is worth taking information warfare seriously, particularly as it affects critical national infrastructures and one's own information resources—not because a catastrophic attack is inevitable, but to prepare for an uncertain future.

Notes

* Dorothy Denning, *Information Warfare and Security* (New York: Addison Wesley/ACM Press, 1999)

1. Graeme Browning, "Counting Down," *National Journal* 16, 19 April 1997, 746–49; *Associated Press*, 23 March 1997; "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," US General Accounting Office, GAO/AIMD-96-84, May 1996, 25; Jack L. Brock, Testimony in Hackers Penetrate DOD Computer Systems, Hearings before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, United States Senate, 20 November 1991.

2. Gina Smith, "Hackers Could Switch Toothbrushes for Bullets," *ABC-News.com*, 18 November 1997.

3. Communication from Eugene Schultz, 15 May 1998.

4. Graeme Browning, "Counting Down," 746–49; *Associated Press*, 23 March 1997; communication from Eugene Schultz, 15 May 1998.

5. Communication from Eugene Schultz, 15 May 1998.

6. Erik Kirschbaum, *Reuters*, Bonn, 17 November 1997.

7. *Associated Press*, New York, 30 April 1998.

8. John Diamond, "CIA Seeks to Provide Warnings of Global Conflicts," *Associated Press*, 27 December 1997.

9. Bruce Kammer, "Information Warfare: The Revolution in Military Affairs and How the US Is Adapting to the Future of Warfare," term paper for COSC 511, Georgetown University, 1 May 1997, citing Norman Friedman, *Desert Victory: The War for Kuwait* (Annapolis, MD: United States Naval Institute Press, 1991), 172–78.

10. Kammer, citing United States Department of Defense, *Conduct of the Persian Gulf War: Final Report to Congress* (Washington, DC: Government Printing Office, 1992), 91–94.

11. Kammer, citing Michael J. Mazarr, Don M. Snider, and James A. Blackwell Jr., *Desert Storm: The Gulf War and What We Learned* (Boulder, CO: Westview Press, 1993), 106–07.

12. Alan D. Campen, "IRAQI Command and Control: The Information Differential," in Alan D. Campen, editor, *The First Information War* (Fairfax, VA: AFCEA International Press, 1992), 171–77.

13. Heather Yeo and Hadley Killo, The Evolution of Military Information Warfare, http://www.geocities.com/CollegePark/Quad/8813/main.html.

14. Kammer, "Information Warfare," citing Friedman, *Desert Victory*, 172–78.

15. Winn Schwartau, Information Warfare, 2nd ed. (New York: Thunder's Mouth Press, 1996), 426–35.

16. Chuck de Caro, "Softwar," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, eds., Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA International Press, 1996), 203–18.

17. Chad R. Lamb, "Military Psychological Operations," term paper for COSC 511, 4 May 1997, citing Stephen T. Hosmer, *Psychological Effects of US Air Operations in Four Wars* 1941–1991 (Santa Monica, CA: Rand, 1996), 149–50.

18. Kammer, "Information Warfare," citing Philip M. Taylor, *War and the Media: Propaganda and Persuasion in the Gulf War* (Manchester, England: Manchester University Press, 1992), 235.

19. Chuck de Caro, "Softwar," in *Cyberwar*, 203–218.

20. "Psychological Operations/Warfare," http://www.geocities.com/Pentagon/1012/psyhist.html; Chad R. Lamb, "Military Psychological Operations," term paper for COSC 511, 4 May 1997, citing Stephen T. Hosmer, *Psychological Effects of US Air Operations in Four Wars 1941–1991* (Santa Monica, CA: Rand, 1996), 143–148.

21. Lamb citing Hosner, 143–48.

22. "Psychological Operations/Warfare," http://www.geocities.com/Pentagon/1012/psyhist.html.

23. Lamb, "Military Psychological Operations," citing Hosmer, *Psychological Effects of US Air Operations in Four Wars 1941–1991*, 143–48.

24. Lamb, citing "US Army Special Forces: The Green Berets—US Special Operations Command: Psychological Operations," http://users.aol.com/armysof1/PSYOPS.html.

25. "Psychological Operations/Warfare," http://www.geocities.com/Pentagon/1012/psyhist.html.

26. Mark R. Jacobson, "War in the Information Age: International Law, Self-Defense, and the Problem of 'Non-Armed' Attacks," The Ohio State University, citing Briefing by Martin S. Hill at the Worldwide PSYOP Conference, November 1995.

27. John Rendon, "Mass Communication and Its Impact," in *National Security in the Information Age*, James McCarthy ed., Conference Report, US Air Force Academy, 28 February–1 March 1996.

28. Jim Hoagland, "How CIA's Secret War on Saddam Collapsed," *Washington Post*, 26 June 1997, A21.

29. Tim Weiner, "Iraqi Spies Know U.N. Inspectors' Next Moves, Officials Say," *New York Times*, 25 November 1997.

30. Weiner.

31. Weiner.

32. "Israel Catches Iraqi Agents," *Intelligence Newsletter* 324, 4 December 1997.

33. Michael Evans, "American Spies in the Sky Keep Watch on Regime," *The Times*, 26 February 1998.

34. "UN Inspectors: Iraq Hiding Weapons," *Associated Press*, 4 June 1998.

35. John M. Goshko, "Iraqis May Be Acting to Avoid Surveillance," *Washington Post*, 6 November 1997, A1.

36. Patrick G. Eddington, "Information Should Be Main Target in Iraq," *Navy Times*, 23 February 1998.

37. “Iraq Blames Sanctions for Deaths,” *Associated Press*, 30 November 1997.

38. “Iraq Accuses US of Plotting to Plant Fake Germ Warfare Evidence,” *Boston Globe*, 12 December 1997, A5.

39. Jorgen Wouters, “Magical Mystery Tour,” *ABCNews.com*, 19 December 1997.

40. *Associated Press*, Iraq, 13 March 1998.

41. *Associated Press*, Iraq, 18 March 1998.

42. Winn Schwartau, *Information Warfare*, 2nd ed. (New York: Thunder’s Mouth Press, 1996), 12.

43. Department of Defense Directive S-3600.1, Information Operations, 9 December 1996; see also *Information Assurance: Legal, Regulatory, Policy and Organization Considerations*, 3rd Edition, Joint Chiefs of Staff, Department of Defense, 17 September 1997.

44. Loyal Rue, *By the Grace of Guile: The Role of Deception in Natural History and Human Affairs* (New York: Oxford University Press, 1994), 120–22.

45. Rue, 120–22.

46. “Risky Business: The Threat from Economic Espionage,” video, The National Counterintelligence Center, 1997.

47. David Kahn, *The Codebreakers* (New York: Macmillan 1967), 75.

48. Kahn, 83–84.

49. For a brief history of the Internet, see Peter J. Denning, “The Internet after Thirty Years,” in Dorothy E. Denning and Peter J. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws* (New York: ACM Press, Addison-Wesley, 1997), 15–27.

50. *NUA Internet Surveys*, Review of 1997, 5 January 1998. For the latest figures, see http://www.nua.ie/surveys/how_many_online.html.

51. Jennifer Lenhart, “Keeping an Electronic Eye on the Kids,” *Washington Post*, 29 May 1998.

52. Alex Cohen, “Net Politics: A Mover, but Not a Shaker,” *Wired News*, 8 April 1998.

53. John Petersen, “Information Warfare: The Future,” in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds., *Cyberwar*, *219-226.*

54. Christopher Paul and Miriam Matthews, *The Russian “Firehose of Falsehood” Propaganda Model* (Santa Monica, CA: RAND Corporation, 2016).

Chapter 8

Information Operations in Large-Scale Combat Operations—Operation Iraqi Freedom I

Colonel (Retired) Carmine Cicalese

> *Every DOD [Department of Defense] action that is planned or executed, word that is written or spoken, and image that is displayed or relayed, communicates the intent of DOD, and by extension the USG [United States Government], with the resulting potential for strategic effects.*[1]

As of this writing, it has been 15 years since the Iraqi invasion, and nearly as long since the US Army trained for high intensity conflict or large-scale combat operations. While the Mission Command Training Program Warfighter Exercises are able to generally replicate kinetic conflict with objectively quantifiable results, higher echelon exercises and simulation have not yet matured to the point that information operations (IO) actions, and their resulting effects on adversary decision making, are equally quantifiable or translatable to practical lessons learned. As a result, the Army lacks recent, relevant experience or tested command competence to plan and execute essential IO in large-scale combat operations.

Information is an element of national power that creates, strengthens, and preserves favorable conditions. Given that the United States goes to war as an extension of politics to impose its policies by threat or use of violence, legitimacy is a key factor and dependent on the audiences. Information is an element in unified action and is integrated with other instruments of national power to advance and defend US values, interests, and objectives.[2] Without being mutually supportive, legitimacy becomes at risk or violence becomes preeminent.

IO was a vital part of the Coalition's defeat of the Iraqi military, and its neutralization and ultimate destruction of the Saddam Hussein regime. IO was also part of the collective failure to rapidly stabilize post-invasion Iraq, or deter the emergence of intra-ethnic conflict and an active, externally supported insurgency. While IO has not proven to be a proverbial "silver bullet" to success in today's complex operating environment, it is also undeserving of primary blame when an adversary or other target of IO action fails to respond as desired. Indeed, these are maneuver failures and overall Unified Action failures as much as they are specific IO failures, and frequently attributable to a larger inability to sufficiently harmonize

and publicly contextualize our actions and overall message from the strategic to tactical echelons.

This chapter will discuss how IO was planned by the Combined Force Land Component Commander (CFLCC) and executed by subordinate forces; discuss lessons learned to include how incomplete efforts led to challenges for the occupation; and end with an examination of how the Army can successfully enact information as a warfighting function in future large-scale combat operations. However, before going into detail on IO and Operation Iraqi Freedom (OIF), it is necessary to baseline understanding of what information operations is, and also additional reasons why it is a challenge to integrate properly.

Part of IO's inconsistent application stems from a multitude of doctrinal changes leading to a general lack of common IO understanding across the Army. From 2002 to present, the Army changed its definition of IO several times, including a period when the Army defined IO a joint activity while the Army conducted "inform and influence activities." In 2014, General Raymond Odierno, Army Chief of Staff, discontinued inform and influence activities in favor of the joint definition of IO. General Odierno considered IO an operation that needed to be tightly nested within the overall operational concept and conduct of operations. He also saw that IO had practical application for the Army Service Component Commands executing theater engagement and security cooperation plans in support of Combatant Command deterrence missions.[3]

In decisive action, Army forces normally operate as part of a joint force, often within a multinational and interagency environment.[4] Because the joint and Army IO definitions are synonymous, this chapter will utilize the joint and Army IO definition as of June 2018: "Information operations is the integrated employment, during military operations, of information-related capabilities, in concert with other lines of operation, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."[5]

In practice, IO is fundamentally about affecting an adversary or enemy's decision-making, while simultaneously protecting friendly decision-making, whether information quality of availability, thus creating a relative advantage for US commanders. IO integrates information related capabilities (IRCs) that can be generally conceptualized as either affecting information content or information flow. For example, Military Information Support Operations (MISO), Operations Security (OPSEC) and Military Deception (MILDEC) predominantly target the adversary's percep-

tions and cognitive process, with the objective being a response beneficial to US end-states (normally reducing US risk, resources, or both) —information content. Simultaneously, IO coordinates other IRCs like Cyberspace Operations and Electronic Warfare to affect the adversary's ability to collect, transmit, store, or access information that supports effective or timely decision making and battle command—information flow. Each of these IRCs have a similar function to protect friendly forces, either directly or by identifying similar attempts by the adversary.

The purpose of this explanation is not to establish IO primacy over the IRCs but rather to simply acknowledge the long-standing synergy of synchronizing and de-conflicting activities. Indeed, IO is a planning and integration function. It does not possess capability in itself, and only succeeds through open collaboration with all the IRC stakeholders. That said, the integrated application of IRC through the IO function is inherently a commander-centric activity prone to subjective bias, experiences, and understanding.[6] This, more than any other factor, has led to an uneven application of IO over the past 15 years of combat. Quite simply, the commander's understanding of and operational experience with IO invariably influences their guidance and direction to the staff. The ultimate fault for this disconnect is not with IO, but rather with the Army's broader leader development, education, and training processes that fails to equip leaders with a consistent understanding and peacetime training application of IO.

Convoluting this dynamic, many of the IRCs are cloaked in mystery due to their classification requirements. Many IO successes and failures are hidden behind this curtain of secrecy—a curtain that is seldom exposed to the larger Army. So much so, it is difficult to find and discuss Department of Defense (DoD) discreet and acknowledged military deception and cyberspace activities other than for the DoD to admit that, in general, it conducts such operations when it has the proper authorities. Discussing unique IRCs can be as vague as a doctrinal hand wave due to classification levels and perceived "need-to-know" restrictions.

For example, coordinated small arms ground fire disrupted the rotary wing deep attack of OIF I: Did non-lethal suppression of enemy air defense fail to disrupt the voice command nets and data links? The Iraqi Army quit fighting and disappeared into the city population: Did MISO leaflets and tactical net intrusions with messages provide the final push that persuades the enemy to quit fighting? The Iraqi Army misallocated forces north rather than committing them south against the Coalition's main axis of advance: Was there a successful MILDEC plan executed to convince the Iraqi military leadership to commit forces away from the

main coalition attack? While these answers can be discovered with the appropriate clearances and access, IO lessons-learned personnel frequently are not determined to possess a "need-to-know." This chapter will discuss and work through these challenges attempting to use multiple open sources to best account for an action.

The CFLCC IO Mission: "Go Faster"

In response to the terrorist attacks of 9/11, United States Central Command (USCENTCOM) deployed the Third United States Army, "Patton's Own" Headquarters forward to Kuwait to serve as the nucleus of the CFLCC for Operation Enduring Freedom. From Kuwait, CFLCC led the hybrid ground war of conventional and special operations forces in Afghanistan with the 82nd Airborne, Marines, and Special Forces that successfully and quickly routed the Taliban while Osama Bin Laden and other Al Qaeda leaders successfully escaped into the Pakistani Tribal Areas.[7] By April 2002, CFLCC Headquarters was extricating its role as the ground component lead for Afghanistan, and turning over authority to Combined Joint Task Force–180.

Surprisingly, CFLCC was preparing for a second conflict that would be different than Operation Enduring Freedom, and more familiar as a conventional large-scale combat operation for which the CFLCC personnel had trained. The Bush Administration was pressuring Iraq to comply with the United Nations mandate to destroy its inventories of weapons of mass destruction, end support to terrorism, and cease prosecution of its civilian population.[8] Weighing possible military options, the Secretary of Defense summoned CFLCC leaders and planners to the Pentagon for a Joint Chiefs of Staff "Tank" discussion. The "Tank" is a reference to where the DoD leadership gathers for important briefings and decisions. CFLCC planners briefed an operations plan which, in the words of the lead planner, "turns Kuwait into a huge armored parking lot," amassing overwhelming combat power before invading Iraq.[9] Leadership questions oriented on how long it would take to amass adequate combat power, and how to accelerate the timeline. The ubiquitous question "can we go faster?" permeated the discussion.[10]

CFLCC planners returned to Kuwait with the guidance to re-assess the plan and develop more timely alternatives. The planners deliberately developed a flexible option that would afford the president more latitude and not be bound by over bearing military timelines. At first, the plans team struggled to adapt the plan as it tried to identify how to achieve the same goals as the operational plan given the DoD leadership intent to go

faster. Then, Lieutenant General Paul Mikolashek, the CFLCC, offered guidance: "Do what you think you can with what you think you would have."[11] This again created a planning pause until the CFLCC strategic planner recommended planning based off the Time Phase Force Deployment List (TPFDL).

CFLCC had an Army armored brigade from the Third Infantry Division on the ground which could be enough to secure the Iraqi port of Um Qasr. Next, a Marine Division might secure the Iraqi city of An Nasiriyah. The plans team worked its way through the TPFDL. The concept of a "Running Start" plan was born. The plan would pick up that moniker because it did not wait until the optimum force was in place to launch an invasion. As directed, the military timeline would not limit or impinge upon the presidential decision making.

The "Running Start" would continually evolve and become more agile and dynamic by adding and dropping units from the plan and even execution. The USCENTCOM plan focused on decapitating Saddam Hussein's regime as USCENTCOM identified Saddam Hussein as Iraq's strategic center of gravity (COG). In kind, the CFLCC designated the Republican Guard Forces Command (RGFC) as the operational COG. While there was some debate within the CFLCC planning group as to whether the Iraqi military leadership was the operational COG, the planning group concluded that the RGFC had to be rendered combat ineffective to force the Saddam regime to capitulate. Saddam's son Qusay directed the RGFC and the Special Republican Guard protecting the regime. From here, the IO planners and intelligence support team deconstructed the COG.

An Integrating Planning Strategy

When he was the First Cavalry Division Commander, General Dave McKiernan often ended the Warfighter Battle Update Brief with the following guidance to his commanders: conduct aggressive counter-reconnaissance and maintain constant pressure on the enemy. This guidance was not lost on the CFLCC IO planner who hearkened the guidance of his former command and saw information as means to maintain constant pressure on the enemy.

If the CFLCC mission was to defeat the Iraqi Army by focusing on the RGFC, then IO should contribute towards the accomplishment of that end. This is consistent with Unified Action—the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort.[12] To support the invasion and the commander's intent, the CFLCC IO plan used

proven military planning techniques like COG analysis and Information Preparation of the Environment.

Given the previously discussed definition of IO, the IO team was most interested in which RGFC Critical Capabilities relied heavily upon vulnerable information content or information flow. Supported by the 1st Information Operations Command reach-back intelligence support team, the CFLCC IO intelligence planner developed a robust Information Preparation of the Environment (IPE) describing how the Iraqi military information flowed. This analysis included the strategic military telecommunications infrastructure, operational to tactical radio frequency communications networks, plus the RGFC communications. The IPE described how the Iraqi people processed and consumed information and the influence of culture in terms of information context. For instance, the ordinary Iraqis of 2002 did not have consistent access to the Internet while the elite did have access. Radio, print, and word-of-mouth were the most common forms of communications. Saddam's rumor mill ruled the streets.[13]

Non-state controlled television was available to the elite who were allowed television satellite dishes, and to a small minority of Iraqis who were willing to take a chance in defying the regime. A Sunni Muslim minority ruled over a Shia Muslim majority. While Sunni and Shia have much in common, they have their differences in how they practice their religion. In sum, the IPE described the military and civilian information environment regarding how information flowed within the Iraqi military and how information content mattered especially to the civilian Iraqi populace. It was an information overlay upon the physical terrain of the operational environment.

Using the Information Preparation of the Environment and applying Joe Strange's COG methodology, the IO plans team identified the RGFC as having four critical capabilities: fires, maneuver, command and control, and protection. As the IO team further analyzed the critical capabilities, it evaluated which critical capabilities and subordinate critical requirements and critical vulnerabilities were possibly susceptible to IO. Consequently, command and control (C2) and protection were the two critical capabilities that bore the most worthwhile critical vulnerabilities. Maneuver also had common critical vulnerabilities; a military leader gave maneuver directions via C2 means.[14]

Command and control across any military has technical and human aspects: the ability to physical transmit an order, as well as the ability to in-

spire obedience to the order. Similarly, the RGFC C2 had a technological aspect—information flow—and a human aspect—information content—both of which exposed many vulnerabilities. For instance, the RGFC maneuver voice command nets were vulnerable to electronic attack, and the Iraqi soldiers receiving information through command channels were susceptible to the manipulation of information. The CFLCC IO Planners realized that if MISO messages could be synchronized with overwhelming kinetic fires, IO might have the same effect on Iraqi ground forces as it did during Desert Storm.

Regarding protection, the ground air defense units were critical to protecting the RGFC from CFLCC rotary wing deep attacks and the artillery units, which could have also been part of the critical capability shoot, had similar technical and cognitive information vulnerabilities. The CFLCC IO plan directed units and information-related capabilities to mass non-lethal fires directly upon the RGFC and the protecting air defense and artillery fires to disrupt the Iraqi Army's ability to command and control, maneuver, and protect its forces. In terms of the suppression of enemy air defenses (SEAD), the IO plan directed the use of MISO and electronic warfare supported by OPSEC and, when applicable, supporting unique information related capabilities, like cyberspace operations, to disrupt Iraqi Army C2 and degrade their will to fight.

As Sun Tzu wrote, "If you know the enemy and know yourself, you need not fear the result of a hundred battles."[15] While the main part of the IO plan intended to mass information-related capabilities to increase the adversary's friction, the IO team had to acknowledge that IO was critical toward maintaining friendly freedom of action. In this instance, the IO team conducted an internal analysis (i.e. BLUE Forces COG analysis) based on warfighting functions (WfF). For an attacking CFLCC, maneuver was the most critical WfF. First, the IO plan emphasized operations security (OPSEC) and communications security to protect critical information regarding CFLCC timelines and intentions to include routes and timing of ground and rotary wing movements. At that time against the Iraqi military, CFLCC retained an overwhelming advantage in assured and secured communications to include encryption and frequency hopping radios. Similarly, protecting against mass casualty events was important to maintain US political will. So, the IO effort had to support any counter-missile effort that was capable of producing mass casualty events as a result. In hindsight, it would have been appropriate to have a collection plan that placed

a priority on identifying Iraqi Special Forces serving as forward observers for SCUD missile teams to mitigate the threat. In sum, the defensive IO plan assured maintaining freedom of action from adversary intervention.

Because the IO definition is adversary-focused, there is a perception gap as to how IO can affect civilian decision making. Most civilians, in this case, were not adversaries. The prevailing assessment was that many of the Shia Iraqis to the south, for instance, would support Saddam's removal from power. The CFLCC IO plan intended to communicate to the Iraqi people to support Coalition actions by avoiding combat operations. Here, MISO, Civil Military Operations, Public Affairs, and Defense Support to Public Diplomacy would be critical toward communicating with the Iraqi people to stay safe and not interfere with combat operations. The CFLCC IO plan intended to limit collateral damage to the Iraqi communication infrastructure so that the new Iraqi government would be able to communicate to its other echelons of government and the Iraqi people. IO plan branches and sequels included options to use escalating non-lethal capabilities to protect the Iraqi communication infrastructure for future use by the Iraqi people. Information access would be critical to securing the peace.

To put it into Clausewitzian terms, the CFLCC IO for the invasion used the Direct Approach in attacking the adversary's decision cycle and the Indirect Approach in keeping the Iraqi civilians from turning on the Coalition. Or, in a more complete perspective, the IO plan sought to maximize friction for the Iraqi military, especially the RGFC, and minimize friction for Coalition ground forces. The CFLCC IO plan had great breadth because CFLCC would have many different types of Coalition ground forces with a variety of IRCs responsible for covering a tremendous amount of battlespace.

After completing Phase 3 planning, CFLCC took a short break before the CFLCC C9 hosted a Civil-Military Operations (CMO) conference with supporting unit planners. Most planners had a CMO, IO, or PSYOP background and CFLCC had a strategic planner attend to assist in maintaining continuity with the Phase 3 plan. Using a draft Department of State planning strategy, the conference produced Phase 4 objectives and end states to secure the peace. Then, planning concluded, for a time, while CFLCC redeployed back to Fort McPherson, Georgia to prepare for the next possible mission. In October 2002, a CFLCC exercise validated the IO plan.[16]

Planning and Expectation Frictions

During the Phase 3 IO plan internal brief back to the CFLCC planners, a CFLCC logistics planner challenged the IO plans team that attacking the adversary's information cycle, while protecting the CFLCC decision space and keeping Iraqis safe, was not enough if not outright misguided. IO needed to win the Iraqi people hearts and minds. This was not new. Since its inception and mentioned in the introduction, IO has suffered from others viewing IO through a clichéd prism: "winning the hearts and minds," "wagging the dog," or even "mind-trick."

The IO plans team countered. While winning the hearts and minds is often considered an IO specialty, the CFLCC plan had limitations. First, it was inherently challenging to win hearts and minds when the bullets would be flying in a large-scale combat operations (LSCO) context. Secondly, the commander would have to be willing to commit more than just information-related capabilities towards winning the hearts and minds. In most instances, information unto itself is not enough to positively influence people to support a cause. Information requires action or a convincing promise of action. Many Army commanders would learn to appreciate this during the 2007 Surge and counterinsurgency operations. Lastly, and most importantly, the IO plan was singularly focused on facilitating the defeat of the Iraqi military including the RGFC.[17]

By late June 2002, the IO staff and planner had a one-on-one session with the CFLCC over such dissonance. The commander was rightfully ambitious challenging the IO staff to consider how an IO plan might win the battle without firing a shot. The IO team understood that the commander was implying that thoughtful precision application of strategic action synchronized with information-related capabilities could convince Iraqis to take matters into their own hands and overthrow Saddam.[18]

The CFLCC IO plans team struggled to identify the appropriate information-related capabilities and authorities needed to fulfill this rather ambitious objective within the prescribed available time. Often, the identified capabilities and authorities fell outside CFLCC's span of control, and CFLCC planners needed to coordinate capability delivery with owning commands/departments and/or request an expansion of authorities to leverage said capability unilaterally. The IO plans team recommendation to the commander was to keep the people and their communication infrastructure safe during combat operations so the peace could be secured in Phase 4. Still, the CFLCC would continue to press USCENTCOM for more authority.[19] In the end, though, USCENTCOM would retain the stra-

tegic initiative, and use IRCs in a synchronized manner with kinetic actions to compel Iraqis to remove Saddam from power prior to the commitment of Coalition ground forces.

Execution and Innovation

On 19 March 2003, USCENTCOM initiated Operation Iraqi Freedom with coordinated strategic bombing and information activities. "Shock and Awe," as it was coined by the Western media, rained bombs and messaging down on the Iraqi military. The Coalition attempted to decapitate the Saddam regime through precision strikes and messaging designed to reduce Iraq's ability to wage war and establish the conditions necessary to promote regime change from within Iraq.[20]

After the invasion, open source media reports included stories that USCENTCOM sent MISO messages to Iraqi leaders in attempts to influence them to not support and even kill Saddam. The US government never confirmed these stories. If true, though, such IO efforts would have been consistent with the CFLCC guidance to win the fight without firing a shot.

Whereas days of air and indirect preparatory fires preceded the Desert Storm ground invasion, Operation Iraqi Freedom had only a day of preparatory kinetic fires. CFLCC massed its forces along the International border between Kuwait and Iraq. These forces included from east to west: the 1st Marine Expeditionary Force including a Marine Division, a Marine Expeditionary Brigade and a British Armored Division; Fifth United States Army Corps with three Army Divisions—also in play was the 4th Infantry Division awaited equipment landing in Turkey, and US Special Operations Command-Central with multiple task forces. Ultimately, Saddam and his sons were able to maintain their fleeting grip on power prior to the invasion despite CFLCC's coordinated and direct efforts to the contrary. As a result, CFLCC forces crossed the line of departure on 21 March 2003.[21]

It is important to understand that, in 2003, many of the IO staffs were lightly manned, often with people not possessing any IO training or experience. Furthermore, commanders had a variety of perspectives of IO from classical command and control warfare that was designed to create advantages in C2, to influence operations intended to mitigate violence between ethnic groups. Given the breadth of the CFLCC IO plan designed to maintain constant pressure on the enemy, protect friendly decision space and minimize Iraqi civilian casualties, subordinate commanders had to make decisions as to how to best utilize their limited staff and IRCs. CFLCC had an operational approach towards the application of IO, while each of

the CFLCC subordinate commands took an integrated tactical approach tailored to their missions.

By most accounts, the CFLCC invasion crossed the line of departure without incident as the Iraqi military may have expected a longer preparatory fire barrage as witnessed during Desert Storm. On 26 March 2003, the 173rd Airborne brigade conducted an airborne operation in northern Iraq that met no organized resistance from the Iraqi Army. The ground operations were over in less than two months.[22] Other than some unexpected resistance from the Fedayeen, to discuss later, all indicators pointed to the fact that CFLCC had successfully protected its decision space.

As CFLCC forces made progress, CFLCC IO was successful in shaping the operational environment through the information environment. MISO, nesting with the Shock and Awe narrative, was hugely successful in degrading the Iraqi military's will to fight. This was a tiered approach. CFLCC and immediate subordinate headquarters nominated targets and messages for delivery by air assets. The coalition dropped millions of leaflets upon Iraqi RGFC and army forces imploring them to not fight. MISO messages ranged from questioning the value of Iraqis fighting for Saddam, to how the Iraqi military should properly park armored equipment. Other messages highlighted Saddam and his sons' ostentatious lifestyle to separate the rank-and-file of the Iraqi military from its leadership.[23] Meanwhile, tactical MISO teams used loudspeakers to encourage forces in contact to surrender.[24]

As the saying goes, the enemy gets a vote. While the RGFC may have been the COG that CFLCC identified, Saddam's Fedayeen gave the most resistance and arguably impeded progress more than the RGFC. For several days, the Fedayeen delayed 3rd Infantry Division's (3ID) advance inflicting casualties and disrupting Coalition logistics forces. In late March 2003, a misoriented logistical convoy would suffer deaths and the Coalition's first prisoners of war. Within days, a Special Forces team would rescue Private Jessica Lynch from the hospital using helmet camera to video tape all of it including a team member presenting Private Lynch with an American flag to soothe the Soldier's nerves. The video images of American Special Forces rescuing Private Lynch gave some ease to an anxious American public and military concerned for their Prisoners of War. The Iraqis, to their credit, highlighted the humane treatment they gave the unguarded Soldier at the hospital.[25]

Within a week, 3ID defeated the outgunned Fedayeen and continued north. This begs the question, though, would a dedicated and loyal Fed-

ayeen been as susceptible to Coalition MISO as the RGFC seemed to be? Furthermore, the Fedayeen fought more like a guerilla organization than the traditional military organization so its communications networks may not have vulnerable as were the RGFCs.

As 3ID advanced, the RGFC had two divisions waiting at the Karbala Gap—critical terrain that defended the high-speed avenues of approach towards Baghdad. The Battle of Karbala offers a few instances of IO execution. As discussed, the CFLCC IO plan included coordinating IRCs as part of SEADs to support rotary wing attacks. Before the 3rd ID tanks arrived at the Karbala Gap, the 11th Aviation Regiment launched a rotary wing deep attack against the Medina Division. By deploying civilian forward observers using cell phones and hand-held radios, the Iraqis successfully thwarted the attack damaging several helicopters and resulting in the Iraqis capturing two US Apache helicopter pilots. The pilots would later be freed without harm.[26]

There were several factors that contributed to the Aviation Regiment's challenges. It is possible this was also an indication the non-lethal SEAD may not have been adequately planned. By 2003, the Army had divested itself of the bulk of its organic Electronic Warfare capabilities and expertise, so the Army lacked both the capabilities and capacity needed to unilaterally suppress enemy air defenses to enable the 11th Aviation Regiment's deep attack. Compounding this macro-level issue, the few IO personnel in theater that did possess the requisite expertise to effectively plan and integrate electronic warfare were not present in the 11th Aviation Brigade's planning efforts prior to the attack.

While OPSEC was successful in protecting the invasion timing, it could not protect all elements of deployment information. This may have contributed to the array of Iraqi forces in Karbala. According to open source reports after the Battle of Karbala, the threat of 4th Infantry Division (4ID) invading from Turkey convinced Qusay Hussein to redeploy a depleted Republican Guard Corps from Karbala to north of Baghdad. This reduced the enemy armor presence at the Karbala gap that would allow unprotected 3rd ID to promptly defeat the Median Division, pour through the gap and race to Baghdad unimpeded.

Many Iraqi soldiers simply chose not to fight and went home, but not the way CFLCC expected. Persistent MISO messaging gave specific instructions on how the armored formations should array their vehicles to depict surrender, and how the Iraqi soldiers should present themselves to the Coalition for surrender. Instead, the Iraqi Army just abandoned most of

their vehicles and faded back to civilian life with their individual military issued side arms. After the Battle of Karbala, there were very few instances where the RGFC offered organized resistance.

Once 3ID passed through the Karbala Gap, the RGFC forces arrayed around Baghdad were mostly empty vehicles. One Iraqi unit did successfully resist for a while near Baghdad Airport before relenting to a 3ID Thunder Run through downtown Baghdad. As one RGFC general pondered after the battle of Baghdad airport:

> The percentage of forces that really fought was simple. I don't have exact numbers, but I can say almost 15 percent. In spite of that, it kept on fighting for three weeks—so what if everybody was fighting? We might have fought for longer time, and we could have delayed the enemy and forced him to pay heavy price, so as to have justice for the Iraqi people and armed forces from historic point of view?[27]

CFLCC forces had many other instances of executing the IO plan to include their own adlibbing and originality. In the Shia holy city of An Najaf, an element from the 101st Airborne Division surprised the Najaf citizenry when they appeared in the city square. A quick-thinking commander told his troops to take a knee and point their weapons at the ground while the commander and his translator spoke to a local cleric. The situation quickly diffused and the coalition avoided offending any Shia religious leaders. If anything, this singular event set the tone that demonstrated that the Coalition's valued and respected Iraqi beliefs, customs, and institutions. Meanwhile, a Marine detachment to the east in Um Qasr led Iraqis in a cheer for Iraq with the event captured on television.

The most far-reaching IO action of the invasion came from a tactical MISO team assigned to the 1st MEF. After 3ID's famous "Thunder Run" concluded and the Iraqi Army disappeared into the night, an M88 armor wrecking vehicle and the tactical MISO team found itself in Firdos Square (not far from Saddam's statue towering over the square). Noticing the Iraqis feeling emboldened enough to defame Saddam's statue, the tactical MISO team used loudspeakers to compel the Iraqi crowd to assist as the M88 tore down Saddam's statue. The Iraqis frolicked on the befallen image of Saddam, throwing their shoes at it.[28] The resultant images sent a very clear strategic message: Baghdad was no longer Saddam's city. Although, more than one media outlet claimed it to be a staged event.[29]

The CFLCC plan called for the protection of the Iraqi communication infrastructure. To make this happen, commands had to submit rec-

ommendations to higher headquarters to maintain a restricted target list. This required diligence and negotiations with other headquarters to convince them, for example, to not destroy a bridge that has a telecommunication line running through the infrastructure of the bridge itself. Likewise, CFLCC had to offer non-kinetic alternatives which could degrade, disrupt, neutralize, or otherwise deny a target.

Perhaps the best instance of this was how the Coalition handled Saddam's ubiquitous spokesman Muhammed Saeed al-Sahhaf (aka Baghdad Bob). Saeed had a perpetual TV presence, adamantly denying any and all coalition progress. Night after night, he appeared unfazed of any impending coalition action. The coalition tried several non-lethal options to deny Baghdad Bob from transmitting having some success in forcing him to move. Eventually, the Coalition physically destroyed the transmitter to neutralize the Iraqi Government's primary means to propagate itself to the outside world.

Lastly, the CFLCC plan to protect the Iraqis non-combatants had mixed results. In general, there were few media accounts of collateral damage or Iraqi civilian deaths due to ground operation during the forty-five days of combat. This did not mean, however, that Coalition operations did not create any civilian casualties. Iraqi civilians died. Plus, there were some instances of concern that could affect a future peace. During the initial push through southern Iraq, Civil Affair teams reported meeting Iraqis who said, "Thank you, now leave."[30] This indicated that the Coalition to include CFLCC may not have fully understood the tensions within the country.

Immediately after combat operations, Frontline documented a tank squad destroying an Iraqi man's vehicle because he was allegedly stealing wood and his child was not enrolled in school. While the Soldiers promptly faced disciplinary actions, the damage was done. Such actions do not win hearts and minds if that is what IO is supposed to do. On the other hand, one could argue it was tactical level Shock and Awe, just not the kind of Shock and Awe CFLCC wanted.

Conclusion

While there is no limit to the IO lessons learned, the most important lessons involve tiered coordination, the precursors of what would become CEMA, and post combat operations planning. CFLCC was two headquarters removed from its next closest subordinate command which created an environment where it was easy for higher headquarters to defer too much action to the subordinate headquarters such that higher is only a

pass-through command. This would not be acceptable. For instance, CFLCC had to manage MISO leaflet drop and broadcast target nominations. Amidst coordination, all units need to have cognizance of what higher and lateral are doing with information such that there is trust that the lowest headquarters doesn't have to do it all. This allows each headquarters to manage its limited IRC assets and nest efforts to achieve synergy.

In another instance, it is easy to argue whether the approach of applying IRCs to disrupt the adversary's air defense has merit. After all, CFLCC itself might not directly oversee an attack involving rotary wing aircraft so how can CFLCC force a subordinate unit to plan and execute a proper non-lethal SEAD? Also, subordinate Army units might not have the necessary skilled personnel to do all of this. At least, though, the guidance assists subordinate commands with priorities and focus.

With regard to SEAD planning, the advent of CEMA and renewed emphasis on assigning EW personnel to army formations should improve the future success of army aviation. Likewise, the addition of cyberspace operations and personnel to army formations gives the IRCs more capability. This alleviates responsibilities that previously fell on the IO planners and synchronizers. This development could portend the improved future integration of technical IRCs that will enable decisive results against enemy C2.

While Phase IV planning did occur, the strategic decision to not conduct Stability Operations damaged the post-Phase III operational environment. Still, CFLCC and the coalition writ large did not fully understand or appreciate the complexity of the Iraqi information environment, and more so the actors and stakeholders operating within it. Iran was strategically committed to making Iraq a weak state from which it could forward project its influence regionally. Given the overwhelming number of Iraqi Shia to Iraqi Sunnis and their proximity to Iran, Iran had interior lines, not just logistically, but culturally as well that the Coalition could never hope to replicate or consistently interdict. Iran understood the differences between Iraqi Shia and Sunni and how to exploit it.

Information without corresponding action is pointless. Such was the occupation. The coalition said life would be better without Saddam. Yet after a few months, life was not improving. Crime was rising and the society was falling apart. The coalition told the Iraqi military Saddam was not worth fighting for and to go home with honor. Then, the Coalition Provincial Authority fired them. With honor lost and the Iranian backed Shia killing Sunni Baathists, the Sunni options were to fight, flee, or do nothing.

CFLCC's IO plan worked mostly as intended. Inevitably, though, the invasion itself mired in a deliberate lack of afterthought and decisions made at strategic levels. The lack of coordinated message to action in Phase III led to the inexorable slide towards a counter-insurgency. Many of the information principles of a counter insurgency, like coordinating message to action, using information to find high value targets, and so forth, apply to large-scale combat operations but differ in scale.

The importance of successfully managing and manipulating information in the 21st Century's Information Age cannot be overstated. The chapter's opening quote from the National Defense Strategy highlights the importance of information. Plus, the Secretary of Defense has produced more guidance for information. In the 2016 "Department of Defense Strategy for Operations in the Information Environment," Secretary Ashton Carter avers: "Information is such a powerful tool, it is recognized as an element of US national power—and as such, the Department must be prepared to synchronize information programs, plans, messages, and products as part of a whole of government effort."[31]

This DoD guidance set the table for Secretary Mattis to approve the Information Joint Function which is a superior intellectual model to IO that fully captures the breadth, diversity and importance of information to warfighting. The Information Joint Function is not bound to just the adversary but influences all relevant actor perceptions and behaviors. Indeed, the relevant actor's behavior is more important than the actor's perception. Moreover, information is vital to human and automated decision making. The human aspect and the human reliance on technology are inseparable.

The 2018 National Defense Strategy acknowledges the changes information and associated technology as it notes the use of emerging technologies to discredit and subvert democratic processes in Georgia, Crimea, and eastern Ukraine is concern enough.[32] From actions in Ukraine to the South China Sea, US competitors recognize that information is a weapon.

The US military must adapt more quickly to this changing environment and fully adopt information as a way of fighting war. To do less is to cede the space to a capable, agile, and willing adversary who wants to win as much as the US military hates to lose.

Notes

1. James Mattis, "National Defense Strategy, 2018," 2, accessed 8 July 2018, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2. Mattis, "National Defense Strategy, 2018," I-14.

3. Matthew J. Sheiffer, "US Army Information Operations and Cyber-Electromagnetic Activities: Lessons from Atlantic Resolve," *Military Review*, 19 March 2018.

4. Headquarters, Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC:) 2-1.

5. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: 2012).

6. FM 3-0, *Operations*, 2-24.

7. Army Central Command ARCENT, accessed 8 July 2018, https://www.globalsecurity.org/military/agency/army/arcent.htm.

8. George W. Bush, "Remarks by the President in Address to the United Nations General Assembly, New York, New York," official transcript, press release, 12 September 2002, accessed 8 July 2018, https://georgewbush-whitehouse.archives.gov/news/releases/2002/09/20020912-1.html.

9. Lead CFLCC Planner, Name Unknown, Remarks to the CFLCC planning team upon returning from the tank session, April 2002.

10. Colonel Carmine Cicalese, "Firsthand experience while serving as the CFLCC IO Planner, April 2002 to July 2002."

11. Cicalese, Firsthand experience.

12. FM 3-0, *Operations*, 2-1.

13. Cicalese, Firsthand experience.

14. Joseph Strange, "Center of Gravity & Critical Vulnerabilities," Marine Corps University, Quantico, VA, 1996.

15. Sun Tzu, *Art of War*, (Hollywood, FL: Simon and Brown), 2011.

16. Kevin Cavanaugh, CFLCC PSYOP Officer email note to Major Carmine Cicalese circa November 2002.

17. Carmine, Cicalese, "Redefining Information Operations," *Joint Forces Quarterly*, 69, 2013.

18. Cicalese.

19. Cicalese.

20. David Martin, "Iraq Faces Massive US Missile Barrage," *CBS News*, 24 January 2003, accessed 8 July 2018, https://www.cbsnews.com/news/iraq-faces-massive-us-missile-barrage/.

21. Gregory Fontenot, et al, *On Point. The United States Army in Operation Iraqi Freedom*, (Fort Leavenworth, KS: Combat Studies Institute Press, 2004), 441–496.

22. Fontenot, *On Point*, 441–496.

23. "Operation Iraqi Freedom," *Conflict 21*. United States Air Force, 13

March 2006, accessed 8 July 2018, http://c21.maxwell.af.mil/iraq.htm#willing.

24. Sergeant Major Retired Herb Friedman, "Operation Iraqi Freedom," accessed 8 July 2018, http://www.psywarrior.com/OpnIraqiFreedom.html.

25. Helen Kennedy, "RESCUE POW IN DARING RAID Supply clerk found wounded at hospital," *NY Daily News*, 2 April 2003.

26. Colonel David Eshel, "Deadly Scourge of the US Helicopter Pilots in Iraq," Defense Update, 10 February 2007, accessed 8 July 2018, http://defense-update.com/20070210_us-helicopter-iraq.html.

27. Interview with Raad Haamdani, *Frontline*, accessed 8 July 2018, https://www.pbs.org/wgbh/pages/frontline/shows/invasion/interviews/raad.html.

28. Fontenot, *On Point*.

29. David Zucchino, "Army Stage-Managed Fall of Hussein Statue," *Los Angeles Times*. 3 July 2004, accessed 8 July 2018. http://articles.latimes.com/2004/jul/03/nation/na-statue3; Common Dreams, 9 December 2004, accessed 8 July 2018, https://en.wikipedia.org/wiki/Common_Dreams.

30. Mark Shankle, Interview circa 2 April 2003. The 1st Cavalry Division G5 shared a 3ID G5 SITREP with the 1st Cavalry Division IO Officer.

31. Ashton Carter, "Department of Defense Strategy for Operations in the Information Environment, June 2016," 1.

32. Mattis, "National Defense Strategy, 2018," 2.

Chapter 9

The Cyber Crucible: Eastern Europe, Russia, and the Development of Modern Warfare

Wesley P. White

The United States Army is unequivocal in its belief in the importance of cyberspace. The first paragraph in Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*, states that superiority through indirect means (either through cyberspace operations or other electronic warfare) is decidedly advantageous to all commanders at all levels, and that these indirect means will serve as a critical component to future land operations.[1] Though the US Army has recognized the importance of the cyber domain in conflicts going forward, the Russian Federation has delivered a masterclass on the development and integration of cyber capabilities into modern conflicts and seems wholly invested in the idea of cyberspace operations and other indirect actions being a primary means of force projection, rather than a useful (or necessary) pairing with traditional kinetic forces.

In February 2013, General Valery Gerasimov, Russia's Chief of the General Staff (comparable to the US Chairman of the Joint Chiefs of Staff), published an article titled "The Value of Science is in the Foresight," in the weekly Russian trade paper *Military-Industrial Kurier*. In it, Gerasimov suggested that the "very 'rules of war' have changed," and that in many cases, nonmilitary means have exceeded the power and force of weapons in their ability to effect change on the international stage.[2] Gerasimov argues that new technologies have reduced gaps between traditional forces and their command and control, though also noting that "frontal engagements of large formations of forces at the strategic and operational level are gradually becoming a thing of the past."[3] The future, Gerasimov suggests, lies in "contactless actions"—made through cyber or other electronic means—being used as the main means of military or intelligence goals. This belief—that traditional military interactions are giving way to newer and subjectively more effective indirect interactions via computers and electronics—has been dubbed by some as the Gerasimov Doctrine.[4]

The timing of the release and publication of the Gerasimov Doctrine is important. Closely after the release of Gerasimov's article, Russia invaded Ukraine with both tanks and malware. The Russian digital incursion into Ukrainian networks, in tandem with a physical military assault, was something the Russian Federation had been practicing for almost a decade. Targeting Estonia in 2007, Georgia in 2008, and eventually Ukraine in 2014,

these attacks used cyber effects, more traditional effects (with mechanized ground units, troops on the ground, and aircraft), or a combination of both. In each of the three instances, Russian force escalated in both scope and complexity. Russia has set forth the blueprint for the training and development of an effective cyber corps, and broadcast to the world how it has effectively integrated cyber operations with traditional large-scale military maneuvers. Moreover, Russia is making it known how they perceive the place of cyber, and other indirect forms of conflict, as shapers of policy.

From a military perspective, Russia's crawl-walk-run progression of cyber operations—enacted through casual disregard for international norms and standards of conduct—has enabled it to develop its cyber corps through real world cyberspace missions. Russian cyber operators have worked in tandem with Russian military operations to find the most effective ways to integrate cyber effects into more traditional military battlespace. This invaluable experience, unable to be fully recreated in training laboratories and exercises, affords Russia the dual abilities of both shaping and better understanding the battlefield of the future.

Understanding the Terms

Before considering the how cyber operations fit into the current understanding of battlespace, one must ensure that he or she understands at least the definitions of baseline concepts within the cyber domain.

First, this chapter will eschew the term "hacker." "Hacker" is a loaded, ill-defined word; its position as a ubiquitous catch-all for bad actors "on the internet" necessarily means it should be excluded from a more granular discussion of cyberspace operational development. Because the concepts dealt with herein deal more with nations and nation-states, the term "attacker" is more appropriate.There are two types of actions to delineate for the purposes of this chapter: cyber-attack and cyber-warfare. A cyber-attack must aim to undermine the function of a computer or computer network and must have a political or national security purpose.[5] A generic end user being infected with malware from a bad website is not a cyber-attack. Further, state or non-state actors may propagate a cyber-attack. Richard A. Clark, former member of the US National Security Council, defines cyber-attacks as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption,"[6] and Michael Hayden, former Director of the National Security Agency, describes cyber-attacks similarly as a "deliberate attempt to disable or destroy another country's computer networks."[7]

On a larger, purely nation-to-nation scale, is cyber-warfare. Cyber-warfare will also always meet the benchmarks of a cyber-attack, though not all cyber-attacks are cyber-warfare. A cyber-attack rises to the level of cyber-warfare—that is, the "level of an armed attack justifying self-defense under Article 51 of the U.N. Charter"—when the attack results in physical destruction comparable to a conventional, kinetic effect.[8] If an attacker launches a denial-of-service attack against a telecommunications provider or datacenter, for instance, this would not rise beyond the definition of cyber-attack; however, if the attacker unleashes malware which destroys stored data, device firmware, or information back-ups, those events would be more in-line with "cyber-warfare."

With that said, where else should the Gerasimov doctrine—a doctrine of increased belligerence and warfare through indirect means and "contactless actions"—be eventually aimed but at the North Atlantic Treaty Organization (NATO), Russia's trans-Atlantic menace which too often stands in the way of Moscow's Russo-centric policies?

NATO is based on the concept of collective defense that enhances its strategy of deterrence. Through formal agreements and long-standing and extensive collaboration, NATO sends a strong signal that member states will stand together in the face of threats to deter aggression against its members. NATO exists to preserve the peace and to make sure that changes to the status quo in Europe occur through political processes that lead to the spread of democracy, the rule of law, and adherence to international norms.

To achieve its varied Russo-centric objectives, Russia opted to pick a course of action not to defeat NATO, but to defeat NATO's strategy. By presenting the Western alliance with actions that produce minimal death and minor (if any) physical destruction, Russia has attempted to shift the responsibility of escalation onto NATO, attempting to goad the defensive alliance into launching a pre-emptive attack in order to keep the status quo.[9] If, through ambiguously legal actions, Russia could goad NATO (or simply a NATO-aligned country) into a traditional, military response, Russia could claim to be the wronged, vulnerable defender now suffering an act of aggression—merely because there is no concrete international understanding of when and where a military response is appropriate for a cyber-attack.

Estonia

The attack on Estonia was a two-phase offensive. Initially, the attackers engaged in little more than electronic vandalism, such as hacking into

the website of the political party that led Estonia's coalition government, where the attackers posted a fake letter of apology from Prime Minister Andrus Ansip for moving a statue. In the second phase, the attacks escalated into a full-scale campaign. The aim was to overload Estonia's computer servers with massive volumes of message traffic causing them to crash, leveraging bot-nets—large networks of computers which have been taken over by malware and which are controlled from one or more central locations—to bombard the targeted Estonian systems with millions of fake messages. Some estimates suggest that one million computers were co-opted or otherwise employed globally for this Distributed Denial of Service (DDoS) onslaught on the servers of a country of 1.3 million inhabitants.[10]

Georgia

Cyber-attacks on Georgian systems were already under way before Russia invaded in 2008. On the day the ground attacks began, sites such as stopgeorgia.ru posted lists of Georgian targets to attack as well as instructions on how to launch those attacks.[11] While Moscow baited Georgia with troop movements on the borders of the breakaway provinces of Abkhazia and South Ossetia, bot-nets were already on the attack, degrading Georgian websites, including the pages of the president, the parliament, the foreign ministry, and news agencies. Banks, which were also targets of cyber-attacks, shut down their servers at the first sign of attack to pre-empt identity or monetary theft.[12] This was the first (recognized) time Russian cyber and traditional military attacks were performed in coordination.[13]

Target surveys, targets, domains, and instructions were ready to go and posted to the internet in accompaniment with the initial Russian incursion into Georgia. This was not a fly-by-night operation set up by helping hacktivists; rather, the timing suggests this was a state-sponsored, military-ordered cyber incursion specifically designed to be launched in tandem with the military operation.

Ukraine

Some suggest that Russia is using Ukraine as a perpetual cyber-war testing ground, or as *Wired* described it in a lengthy and detailed report on the matter last year, "a laboratory for perfecting new forms of global online combat."[14] A digital army has systematically undermined practically every sector of Ukraine: media, finance, transportation, military, politics, and energy. Seemingly unstoppable intrusions deleted data, destroyed computers, and in some cases paralyzed organizations' most basic functions.[15] There is no way to know exactly how many Ukrainian institutions

have been hit in the escalating campaign of cyber-attacks, and any count is liable to be an underestimate. For every publicly known target, others have not admitted to being victimized. Still more have not even discovered the intruders in their systems.

The attackers' intentions can be summed up in a single Russian word: *poligon*, translated loosely as "training ground." Even in their most damaging actions, the attackers never seem to go *too far*; the attackers could have knocked out Ukrenergo's transmission station for longer or caused permanent, physical harm to the grid, but instead settled (repeatedly) for blackouts.[16] The attacker never seem committted to full destruction of their targets in Ukraine. Instead, the attackers cease before delivering irreparable damage, playing their cards close to their chest as if reserving their true capabilities for some future operation—one can almost think of it as game planning during a pre-season football game.[17]

The attacks on Estonia, Georgia, and the Ukraine, while highlighting the fusion of cyber-effects with more traditional military operations, should also serve as a wake-up call to military and security circles in NATO nations on both sides of the Atlantic and to highlight questions in need of thoughtful consideration: namely, what are the lessons to take away from the Russian Federation's increased utilization of the cyber domain in their combat operations, and how does this help to shape the battlefield of the future?

Analysis

The cyber domain offers an increased latitude of action for commanders in the modern battlespace in part due to the fog of uncertainty that surrounds the proportion, suitability, and overall effectiveness of responding to a cyber-attack. An attack on a base which wounds and kills opposing soldiers or physically destroys infrastructure may invite a response in-kind, where a communications system that has been denied service or otherwise degraded may not elicit a physical strike in retaliation. Cyberspace operations serve as an excellent avenue of force projection without putting Soldiers in harm's way; these operations have increased the latitude for action in the same way that the development and fielding of the Unmanned Aerial Vehicles (UAVs) did. A UAV can be sent on a mission that may be deemed too hazardous or not important enough to send Soldiers into the field to risk life and limb to accomplish. The same concept applies to a cyberspace operation—rather than send a team into a known hostile area to physically retrieve and return intelligence from an enemy's digital devic-

es, it is easier (and may make more sense) for the commander to approve a cyberspace operation to electronically retrieve the same intelligence.

A cyberspace operation also does not require the complex partnerships that a mission with Soldiers being transported via airplanes, helicopters, ships, or ground vehicles may require. Where a traditional mission may require the use of an airfield in a partner country, or the use of another country's airspace or other violation of territorial sovereignty for the delivery and retrieval of Soldiers and effects, a cyberspace operation is not constrained in the same way. Cyberspace operations may also require significantly less deconfliction to perform than a traditional military operation. There is a far smaller chance of collateral damage coming from a cyberspace operation than through the launching of missiles or dropping of bombs; with that decreased chance of sparking an international incident through harming or killing citizens or soldiers of a different country, an increased utilization of cyberspace operations would allow a commander more avenues to prosecute their target or objective.

The ability to launch a cyber-attack changes the face of a large-scale combat operation because the efficacy of the operation can be wildly out-of-proportion to the risk of damage or loss. When a few strokes on the keyboard—from dozens, hundreds, or thousands of miles away—can turn an enemy's power off, disable their communications, or turn their transportation systems into a chaotic, unmanaged mess, and the cost in lives, equipment, and resources is negligible, then a commander finds him or herself in an advantageous position from which to launch further attacks (cyber or otherwise).

For all the new and exciting avenues open to a commander on the offensive, the introduction of cyberspace operations should also be of great concern. Much of the modern battlespace is shaped by timely—if not instantaneous—communication, and it is exactly that communication which would be targeted by a group waging a cyber-attack. Unfortunately, the best and only surefire way to defend a machine with any sort of connectivity is to disable or unplug it; otherwise, a determined attacker will eventually gain access. He or she only needs to wait for an end-user of that machine or equipment to make the fatal mistake which grants the attacker access. Defensive cyber operations have their place but, due in part to the ever-present risk of human error, serve primarily as a delaying action. What this practically means is that the best defense is a good offense, and that energy should be focused on assaulting any enemy's (digital) position with such overwhelming force and violence that the same force and violence cannot be offered in return. Scenes from Hollywood, with defenders

running to and fro, typing on this terminal or that keyboard to fend off some sort of cyber-attack have no basis in reality; once a machine has been compromised or degraded, it should be effectively considered out of the fight (until properly remediated). Not only has the commander lost that piece of equipment, but now the attackers who had been focused on the now out-of-commission equipment can redouble their efforts against a different target. In a persistent cyber-attack scenario which a commander would find him or herself in a large-scale combat operation, the losses cascade together like so many dominoes, failures and defeats compounding exponentially until the enemy attacker has control of the systems and freedom of movement within.

The binary choice of offense or defense, at least with regards to modern cyber battlefield operations, is an anachronism. The new commander should seek to deny, degrade, or destroy the capabilities of the enemy with whom he is engaged as expeditiously as possible, understanding that his or her enemy is seeking to do precisely the same thing at precisely the same time.

Conclusion

A crawl-walk-run approach through Estonia, Georgia, and Ukraine has lent the Russian cyber-arm a smooth, well-oiled quality; at the same time, the Russian ability to conduct real world operations, absent effective international intervention, external defense, or interdiction has allowed a honing of tactics, techniques, and procedures (or TTPs) and tools to greater obfuscate Russian presence and activity.[18]

Estonia, the initial victim, was a low-key affair, or the crawl: cyber-attacks launched, without being paired with military intervention, which in retrospect can be viewed as a proof-of-concept. Georgia, a step beyond Estonia, was the walk: pre-formed bot-nets sending pre-formed packets, in a larger-scale denial of service attack, but now paired with an incursion of troops and tanks and a traditional military movement into the South Ossetia area. Through postings on various internet forums and sites, paramilitary cyber activity seems to have been, if not encouraged, but also not discouraged—which only served to swell the ranks of those conducting cyber-attacks on Russia's behalf. Finally, Ukraine, was the run: large-scale cyber-attacks paired with military incursion and occupation. Simultaneous attacks occurred on media firms; an attack on the Central Election Commission's website triggered the announcement of an ultra-right-wing candidate as winner of the election; and an incursion took over the networks which connected and controlled the systems for entire power grids.

Once the desired levels of denial, degradation, and destruction had been achieved, the attackers destroyed the firmware for the network cards in the machines, leaving administrators and responders unable to fix the issue remotely.[19]

It is perhaps best to think of the ongoing cyber activity in Ukraine as Russia's Combat Training Center, or CTC. The purpose of a CTC is to provide realistic collective training for Soldiers, leaders, staffs, and units according to Army and Joint doctrine, simulating as closely as possible the rigors and stresses of combat.[20] The CTC ensures Soldiers, units, and leaders are well prepared for current and future operations; no other means of training provides the Army with the ability to maintain the consistently tough and realistic training environment that combatants require for success in warfare.[21] Though cyberspace is a tested domain at both the National Training Center (NTC) and at the Joint Readiness Training Center (JRTC), there is not a dedicated electronic or cyber CTC with which to train US Army (or military at-large) cyber actors.[22] This leaves cyber-training to be conducted in more traditional, lab-based environments, the limitations of which are clear: training networks can only be so large; the trainer can only provide the types of operating systems that he or she has access or license to provide; and the vulnerabilities and/or exploitation vectors provided to train a cyber-actor are limited to what the training facilitator can think of (or knows about) at the time he or she is putting together a network. In the case of Russia, however, adventurism in Ukraine has served to offer a holistically complete training environment for the Russian cyber-forces—state-sanctioned or otherwise. Russian forces will find a width and breadth of computers and operating systems, in a variety of patched and unpatched states, administered by both the lazy and hyper-vigilant. Russian cyber actors can train against medical, transportation, banking, power, or education systems, take note of what works and what does not, and then take that real-time, operational data back to the coders and developers to manipulate their cyber toolkit on the fly, increasing their efficacy for the next round of attacks.

"Russia is not only pushing the limits of its technical abilities," says Thomas Rid, a professor in the War Studies department at King's College, London, "but also feeling out the edges of what the international community will tolerate."[23] The Kremlin meddled in the Ukrainian election and faced seemingly ineffective repercussions; Russian and Russia-aligned actors continue to wreak havoc across the country in a variety of necessary and national-security-level industries, including turning the power off and on in Ukraine with impunity.[24] Then, full of confidence from their eastern

European triumphs, Russia tried similar tactics in Germany, France, and the United States. Russian government cyber actors have targeted "government entities and multiple US critical infrastructure sectors," including those of energy, nuclear, water and aviation, according to an alert issued by the Department of Homeland Security and Federal Bureau of Investigation (FBI).[25] Critical manufacturing sectors and commercial facilities also have been targeted by the ongoing "multi-stage intrusion campaign by Russian government cyber actors."[26] A joint analysis by the FBI and the Department of Homeland Security described the intrusions as extremely sophisticated, in some cases first breaching suppliers and third-party vendors before hopping from those networks to their ultimate target.

Rid suggests that Russia is testing out boundaries and trying to map out red lines; if Russian actions are rebuffed in one area, or an effect that they have produced draws too much attention or creates unacceptable consternation, then Russian forces simply move on to the next target or the next intrusion. However, without significant ramifications—or even merely effective international reaction—Russia may not feel significantly at-risk and, lacking necessary external push back, might continue to the "next step" for their targets.[27] What the escalation of Russian attacks truly suggests, however, is a cyber-war will not be waged at some abstract point in the future; it is happening, at least the initial stages, now, throughout the world, propagated (at least in part) by a seasoned corps of Russian veterans.

Every so often in the history of warfare a sea-change occurs which affects the way militaries function and how combat is conceived. Stone gave way to metal, bows to gunpowder and bullets. Automatic weapons eventually offered commanders a multiplicative increase in firepower and destructive capability. The advent of airpower opened up an entirely new domain on the battlefield, and now the advent of weaponized cyberspace has done the same. The Russian Federation's stepped-inclusion of cyber operations into their military campaigns serves as a proof of cyber operations' utility and benefit to a commander in the modern battlespace. The lesson of Russia's success is not how the Russian Federation developed their program. Instead, having seen the effectiveness that cyber operations can have both in shaping a battlespace and in offering a decided tactical or psychological advantage over an enemy, the lesson is that cyber operations must be more fully integrated into modern combat. Peer and near-peer adversaries alike are fielding cyberspace capabilities and integrating those same capabilities into their operation plans; Russia just happened to display their progression and development on the world stage. With the lati-

tude of action it affords commanders on the ground, the ability to degrade or deny the communications of an opposing force, and the psychological aspect of an effective cyber-attack on the armed forces of an adversarial country (in addition to the population), the cyber domain truly is the next evolution of battlespace. The United States must fully embrace and work to seamlessly integrate cyberspace operations into their plans for combat operations, both large-and small-scale. As has been demonstrated by the Russian Federation's military adventurism through the past decade, the adversaries of the United States fully intend to do just that.

Notes

1. Department of the Army, (FM) Field Manual 3-12, *Cyberspace and Electronics Warfare Operations* (Washington, DC: 2017), 1-1.

2. General Valery Gerasimov, "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." *Military Review*, January/February 2016, 23.

3. Gerasimov, 23.

4. Molly K. McKew et al., "The Gerasimov Doctrine," *POLITICO Magazine*, September/October 2017, accessed 27 April 2018, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538. For the opinion that the Gerasimov doctrine is not necessarily "real," see Roger N. McDermott, "Does Russia Have a Gerasimov Doctrine?" *US Army War College Quarterly Parameters* 46, no. 1, 103.

5. Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," 2012, Faculty Scholarship Series Paper 3852, 836–837.

6. Richard A. Clarke, *Cyber War* (New York: HarperCollins, 2011), 6.

7. Tom Gjelten, "Extending The Law Of War To Cyberspace," *National Public Radio*, 22 September 2010, accessed 15 February 2018, https://www.npr.org/templates/story/story.php?storyId=130023318.

8. Hathaway and Crootof, "The Law of Cyber-Attack," 841.

9. Clarke, *Cyber War*, 34.

10. Robert Mandel, *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*, (Washington, DC: Georgetown University Press, 2017). See also Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence," *Atlantic Council*, 3 January 2014, accessed 20 February 2018, http://www.atlanticcouncil.org/publications/issue-briefs/cybersecurity-and-tailored-deterrence.

11. More than likely, these instructions amounted to having the interested user download a tool such as the low orbit ion cannon, which lets a user opt for their box to be coopted and controlled as part of a larger, Denial of Service or Distributed Denial of Services intent bot-net.

12. John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, 13 August 2008, accessed 13 February 2018, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

13. David J. Smith, "Russian Cyber Strategy and the War Against Georgia," *Atlantic Council*, 17 January 2014, accessed 20 February 2018, http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia. This is more along the lines of what the Rand Corporation was defining as a cyber-attack—computer-based occurrences paired with actual military movements and force.

14. Christopher Miller, "What's Ukraine Doing to Combat Russian Cyberwarfare? 'Not Enough,'" RadioFreeEurope/RadioLiberty, 8 March 2018, accessed 22 February 2018, https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html.

15. Andy Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” *Wired*, 20 June 2017, accessed 14 February 2018, https://www.wired.com/story/russian-hackers-attack-ukraine/.

16. Greenberg, “How An Entire Nation.” “A power company responsible for operational and technological control of the Integrated Power System (IPS) of Ukraine and electricity transmission via trunk power grids from generating plants to the distribution networks of the regional electricity suppliers,” About Us, УКРЕНЕРГО, accessed 7 March 2018. https://ua.energy/about-en/.

17. Greenberg, “How An Entire Nation.”

18. I say “absent effective international intervention” because if the international intervention had been effective, then the cyber-attacks, which still ravage Ukraine, would have been stopped.

19. Greenberg, “How An Entire Nation.”

20. “Combat Training Center Directorate (CTCD),” 8 July 2014, accessed 27 April 2018, https://usacac.army.mil/organizations/cact/ctcd. See also: US Army, “Combat Training Center (CTC) Program 2009 US Army Posture Statement,” accessed 25 February 2018, https://www.army.mil/aps/09/information_papers/combat_training_center_program.html.

21. US Army, “Combat Training Center (CTC) Program.”

22. “Combat Training Center Rotations Continue to Drive Evolution of Army Cyber-Electromagnetic Activities,” *Army News*, 29 June 2017, accessed 26 April 2018, https://www.army.mil/article/190201/combat_training_center_rotations_continue_to_drive_evolution_of_army_cyber_electromagnetic_activitie

23. Greenberg, “How An Entire Nation.”

24. Greenberg.

25. “Alert (TA18-074A).” Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors | United States Computer Emergency Readiness Team (US-CERT), 15 March 2018, accessed 21 March 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A.

26. Jennifer A. Dlouhy and Michael Riley, “Russian Hackers Attacking U.S. Power Grid and Aviation, FBI Warns,” *Bloomberg*, 15 March 2018, accessed March 21, 2018, https://www.bloomberg.com/news/articles/2018-03-15/russian-hackers-attacking-u-s-power-grid-aviation-fbi-warns.

27. Greenberg, “How An Entire Nation.”

Chapter 10

Botnet Evolution during Modern-Day Large-Scale Combat Operations[1]

Lieutenant Colonel Rick A. Galeano, Katrin Galeano,
Samer Al-Khateeb, Nitin Agarwal, and
Lieutenant Colonel James N. Turner

Large-scale combat operations no longer involve only land, sea, and air domains, but also an Information Environment (IE) capable of quickly and unexpectedly changing conditions in all domains within the multi-domain operational environment. A new artificial means, social bots, has been introduced to the constantly evolving IE to shape and influence perceptions and cognitively trigger behavioral change on an exponentially massive scale worldwide. The goal is to influence the IE by amplifying social media followership in the form of "social bots"—scripted codes that mimic human users and serve as super-spreaders of information. These social bots can be used to promote particular points of view, fabricate perception of popularity or popular viewpoint, muddle the discourse and narrative space, and/or serve as a means to bolster these points of view by promoting blogs or other digital content. Effects can range across the physical, cognitive, and informational dimensions to ultimately trigger specific behaviors in individuals and groups that impact the operational environment in a way that is beneficial to those who operate the bots.

For example, in the physical dimension, bots are capable of disrupting infrastructure by overloading networks or hosting platforms with a deluge of information; or they could easily carry obtrusive malware or viruses to deny or degrade a targeted system. Once an infection starts inside a network, it is difficult for network defenders to isolate and contain. Contemplate the potentially catastrophic effect that a Tactical Operations Center's (TOC) mission command systems being denied during large-scale combat operations (LSCO)—where assured communications is vital and may well prove to be the difference between a mission's success or failure. Correspondingly, social bots can shape the informational dimension by corrupting and/or disrupting how information is received, processed, and/or disseminated through mission command systems and human filters—effectively limiting the optimal employment of friendly combat power. Contrary to popular belief effects within the IE are not solely generated through non-kinetic effects; rather "the warfighting functions (particularly movement and maneuver fires) produce effects in the information envi-

ronment, whether intentional or not.[2] Lastly, the cognitive dimension revolves around the perceptions that the audiences receive from any of the messaging and the resultant behavior based on those stimuli. Repeated messaging from what appears to be a variety of independent sources create an echo chamber that focuses on repetition in order to resonate cognitively within targeted individuals or groups. "Rarely does a single tactic, task, method, action, or message change behaviour."[3] Quite simply, the variety employed in disseminating a message and frequency at which that message is disseminated in some cases matter just as much as content itself to generate to required resonance to trigger the desired behavioral change. The case study discussed in this chapter provides empirical evidence in support of this.

The 2014 Russian invasion of Crimea provides a historical case study of hybrid warfare activities involving ground operations and information operations.[4] Social bots operating during this time moved specially-crafted messages through the information environment. Data collected from social media, including blogs and Twitter clearly demonstrate both Russia's intent and capability to manipulate information through the use of social bots.[5] Western analysts utilized socio-computational methodologies to identify the "seeders of information"—sources of information supplying content to the botnets or a set of bot accounts working together—and the communication and coordination strategies used. During the aforementioned event the botnets deployed for propaganda dissemination evolved by becoming increasingly deceptive and well-coordinated to mislead targeted audiences on the direct level of Russian participation and strategic objectives to confuse and delay decision from Western political leaders. This chapter provides the relevancy and importance of reinforcing effects into the information operations domain, especially in the realm of social media, by studying the social network analysis of the effect of hybrid warfare during large-scale combat operations.

What Is a Bot?

A bot is a coordinated computer program that tries to mimic human behavior through messaging/interacting. For example, a bot can manipulate the search results returned by various search engines such as Google.[6] Such methods can be used to elevate a topic into "top trends"—which are often highlighted at the top of search results or social media platforms. This is especially important in today's "Information Age" where many users simply rely on these "top results" to formulate their initial perceptions/positions of a particular event without rigorous examination of all informational sources. In short, the Russians, through their systematic em-

ployment of social bots were able to effectively filter information received by the vast majority of their targeted audiences.

Research shows that most internet traffic, especially on social media, is generated by "botnets."[7] In addition to botnets, the Russians employed large numbers of people to troll social media sites and blogs to disseminate propaganda.[8] The diverse nature of social media user interaction and news distribution creates a huge gap-filled territory for exploitation by social bots and human-bot collaborations that engage in information conflicts, "trolling," or in influencing narratives.

Case Study: The 2014 Crimean Water Crisis

Russia's annexation of the Crimean Peninsula on 16 March 2014 was met with international discontent, and a sense of Russian imperialism to expand their reign of power. Both the United Nations and NATO Secretary General Anders Fogh Rasmussen condemned Russia's blatant aggression and disregard of international law. Grievances, requests for help, and on-the-ground accounts on the developing conflict were reported to worldwide audiences through a variety of open source platforms including blogs, news websites, Twitter, Facebook, and YouTube.

Several stories published by Russian news agencies to mislead and confuse target audiences through the dissemination of disinformation (i.e. lies) and misinformation (i.e. misleading). Examples of these national-level, coordinated efforts include *ITAR-TASS*, which claimed that the Ukrainian government had ceased work on the North Crimean Canal which carries water from the Dnepr River to Crimea.[9] In another example, the Russian international television network Russia Today (RT) reported that satellite images showed Ukraine deliberately trying to cut off the Crimean Peninsula's water supply by building a dam, while Russian scientists were trying to find ways to supply Crimea with fresh water in the meantime.[10] Reliant on these false and misleading stories, a subsequent *New York Times* article reported that a water shortage was observed, Crimean farms were drying, food supplies were inadequate, and the price of basic goods, such as milk and gas, had doubled.[11] All the while, Russian armed forces were fully engaged in LSCO against Ukrainian forces in the eastern Ukraine in July 2014. Russia's employment of new weapons and methods of employment were not limited to non-kinetic capabilities. In eastern Ukraine, an entire Ukrainian battalion was virtually destroyed in four minutes from a barrage of high explosives, cluster, and thermobaric munitions.[12] What remains is clear from Russian involvement in the Ukraine is that they are employing a variety of capabilities in new and

innovative ways to generate a relative edge on the battlefield. The thought that should keep Western military analysts up at night is that the Russians surely did not reveal their full bag of tricks.

Pro-Russian bots leveraged the internet to shape the information environment in the form of echo chambers. "Confirmation bias perpetuates misinformation, and when incorrect information bounces around through an echo chamber, it leaves a mark every place it hits. Even if something we read is disproven, we can't un-see incorrect information."[13] The creators of bots understand the effect of an echo chamber. The low effort and cost combined with the high effect of seeding information through social bots can quickly influence the masses over the short, and in some cases, the long-term. In this case study, these bots were disseminating anti-West and pro-Russian news articles in a bid to create a window of opportunity for Russian forces to achieve their strategic objectives prior to potential Western intervention. Numerous bots were simply tweeting the same article after copying it to various websites and blogs, making it appear as if the articles were independently posted on different website URLs. In other words, bots were cloning the [mis]information, creating an echo chamber and misleading targeted audiences about the military operations that were ongoing in the Ukraine.

Data Description

Often content (e.g., reports, images, videos, and articles) originated from one social media site and were diffused to many other sites without sufficient source attribution. For the purposes of illustrating this point, the authors tracked multiple popular social media sites in an attempt to identify sources and their implicit interconnections. The keywords "Ukraine," "Ukraine Crisis," "Euromaidan," "Automaidan," and "Ukraine's Automaidan Protestors" were used to collect data about the crisis. First, popular blog posts were identified for the Ukraine-Russia conflict, and then cross-referenced these posts with Twitter data to find the posts that were diffused the most on Twitter. Tools such as TweetTracker, and NodeXL were then used to collect Twitter data for the research period between 29 April 2014 20:40:32 and 21 July 2014 22:40:06 UTC—which coincided with [event].[14] This series of methodical queries resulted in 1,361 unique tweets, 588 unique Twitter users, and 118,601 relations (including *follows*, *mentions*, *replies*, and *tweets*) between these users.

Methodology to Identify Botnets

As Russia's strategic objectives and resultant aggression transitioned from Crimea to the Ukraine proper, worldwide media attention did not correspondingly shift. Russia's misinformation efforts played a significant role is this delay. As misinformation continued about the Russian-invented water crisis (just enough information that made it believable), Russian forces—both proxy and conventional—were operating with relative freedom within the territorial borders of the eastern Ukraine.[15]

The hashtag *#Crimea*, in both Russian and Ukrainian language, had erratic results from day to day using the same filtering algorithm. Topics such as *the end of the ceasefire* and *the advance of troops into Southeast Ukraine* began to take precedence. "Propaganda, deception, disinformation, and the ability of individuals and groups to influence disparate populations through social technologies reflect the increasing speed of human interaction."[16] Misinformation promulgated across social channels, keeping all but the outside confused as to what was happening. Controlling this line of communication in the information domain was conducted with an implicit use of narrative control by using botnets. The use of botnets to influence is portrayed in Figure 10.2.

Figure 10.1. Word cloud depicting data description searches of the information dimension related the 2014 Ukrainian water crisis. Graphic created by the authors.

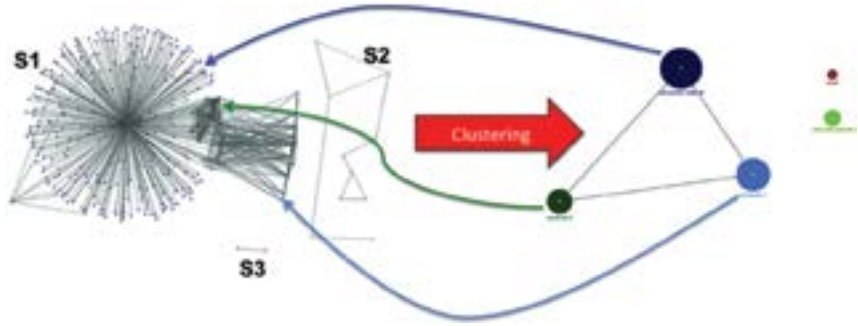


Figure 10.2. Three sub-networks with unusual structural characteristics in S1 are observed when the Girvan-Newman clustering algorithm is applied to the network. On the left are the expanded clusters and on the right is the collapsed view of the identified five clusters. Graphic created by the authors.

The first network that was analysed was the friends and followers network, i.e., the social network. As shown in Figure 10.2, the accounts that were related to the collected data had three sub-networks: S1, S2, and S3. The sub-network S1 exhibited unusual structural characteristics. The other two sub-networks were ignored due to their relatively small size and lack of anomalous behaviors. We applied the Girvan-Newman clustering algorithm—an algorithm that detects communities in a network based on how closely the nodes are connected—and found that the network had five clusters (communities or groups of nodes), as shown in Figure 10.1.[17] The center of the star-shaped cluster within S1 belonged to a "real-person."[18] Figure 10.2 shows the Twitter account, which was connected to 345 bots out of 588 Twitter accounts in this network. **This real person was the owner/operator of a specific webpage that all the other bots referred to in their tweets with different shortened URLs.**

The star-shaped cluster was connected to the other two-syndicate groups, viz. syndicate-1 and syndicate-2. Close examination of these ties revealed that the members of the syndicate groups followed the "real-person" node, and not the other way. The research conclusively determined that "real-person" is the most central node of the entire bot network in question, and functioned as the bots" information source.

The other ties within the two syndicates were mutually reciprocated relationships, suggesting use of the principles "*Follow Me and I Follow You*" (FMIFY) and "*I Follow You, Follow Me*" (IFYFM)—a well-known practice used by Twitter spammers for "link farming," or quickly gaining followers.[19]

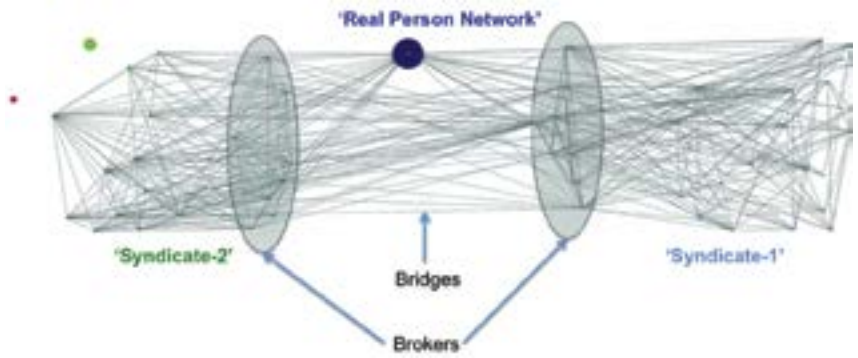


Figure 10.3. This real person network is connected to broker bots that coordinate the dissemination of propaganda through the bots in their respective syndicates. Graphic created by the authors.

Unlike the "real person" network, there is no single most central node in these networks, indicating an absence of a hierarchical organization structure in the "syndicate-1" and "syndicate-2" networks. Further analysis showed that the broker nodes act as interfaces between the group members and other groups. They established bridges that facilitated tweet circulation across the syndicates. The broker nodes were primarily responsible for connecting with the "real person" network, specifically the most influential "real person" node. The operational effect being achieved through this method was narrative control as depicted in Figure 3. Thus Russia, through their use of bot-seeded misinformation, was able to successfully shape the necessary strategic conditions within the IE to allow for large-scale combat operations to begin in eastern Ukraine.

The Military Implications for the Expanded Use of Social Bots

The instantaneous speed and worldwide reach of social media coupled with the quick pace of interactions between a exponentially large set of users, many of whom do not verify the veracity of proffered information and sourcing, create the conditions ripe for the massive manipulation of technologically-dependent societies such as the United States. Quite simply, the more popular a social media message is the more likely non-discerning individuals are to believe that the content is true. This dynamic should not be lost on Western militaries who are beholden to elected individuals that are subject to the approval of their constituencies. The nation's future adversaries and enemies will likely increasingly leverage information as a low-cost and low-risk instrument of national power to corrupt the interconnected tissues of America's "Clausewitzian trinity." At the strategic and operational levels of war, social media platforms that are manipulat-

ed by bots can shift international and regional opinions about the use of military force or validity of military operations in a region. At the tactical level, bot-induced social media propaganda could potentially be used to persuade susceptible targets to disrupt or delay military operations through protests or other "non-lethal" resistance.

Military leaders need to understand that the narrative can be easily manipulated and influenced by bots and trolls. Most users of social media cannot or will not differentiate between real accounts and fake bot accounts. Because social bots can be employed clandestinely in a low-cost, low-risk context military leaders can expect to encounter an increased amount of adversary-generated social media propaganda. Bots will likely be a weapon of choice for America's adversaries and enemies for the foreseeable future.

The growing weaponization of social media is influencing large-scale combat operations. Military units at all levels need to develop tools for identifying threats and opportunities within the IE, and responding to them appropriately across all domains. There is a present need for social media cells that are able to monitor the IE in real-time, and have requisite authorities to pre-emptively act or rapidly respond to adversary actions within the IE. Developing well-trained social media cells at the appropriate tactical headquarters for an operation enables rapid and appropriate response that can neutralize propaganda and mitigate its negative effects.

Three key enablers should be incorporated into Army units to effectively counter bot-enabled social media propaganda. These enablers are Public Affairs (PA), Psychological Operations (PSYOP), and Operations Security (OPSEC). Army Divisions are typically augmented with a Military Public Affairs Detachment (MPAD), a Tactical PSYOP Development Detachment (TPDD), and occasionally an Information Operations Field Support Team (IO FST) in addition to organic support. The MPAD can directly counter bot-enabled propaganda through media engagement and social media outreach. The TPDD can help assess propaganda and evaluate what messages within the propaganda resonate with specific local audiences. The IO FST can manage OPSEC to identify critical information that must be protected to ensure successful operations. All of these enablers must coordinate their efforts to address the threat of bot-enabled propaganda.

Military leaders at all levels must have a broad understanding of the IE, and the potential cross-domain of information. This understanding enables leaders to better incorporate social media considerations into intelli-

gence collection, planning, and operations to best achieve desired effects in an integrated and synchronized manner. Once bots and trolls are identified, Army units can use Public Affairs official social media accounts to counter adversary propaganda by informing interested audiences of the truth so that they can validate this trusted source of information to verify truthful information or debunk myths espoused by propaganda.

Conclusion

Social media use has been shifting from entertainment to public discourse, thereby making it a preferred tool for influencing group opinions or achieving political goals by disseminating propaganda or misinformation about various events. The hybrid warfare observed in Ukraine in 2014 identified how information warfare was successfully employed to support, facilitate, and allow large-scale combat operations; since this time bot networks have evolved into even more complex entities that could exponentially magnify the scale and reach of the effects seen in 2014. A follow-on study conducted by the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS) at the University of Arkansas at Little Rock identified an even more complex series of botnets operating during the 2015 military exercise Dragoon Ride conducted by US Army Europe.[20] These botnets demonstrated a probing attack into the information dimension, the goal was to also change the overall narrative. Although, not included for this chapter, Dragoon Ride 2015 does demonstrate the continued evolution of echo chambers with the use of botnets.

By presenting half-truths, contorted facts, manipulated images, and videos in a cogent manner substantiated by URLs to other propaganda riddled websites, it is not very challenging to mislead a potential target audience, especially during LSCOs—where time constraints make sufficient analysis exceedingly more challenging. Twitter and other social platforms are merely just a mechanism to steer readers in the desired direction. This is where other forms of mass media that allow more expansive content are most helpful to developing a credible story for target audience consumption. Bots are used to steer attention to these blogs. The goal of the bots is to bring the propaganda to as many readers as possible by employing clandestine means as demonstrated in these case studies. Military leaders must consider how they will incorporate information operations to counter adversary use of social media to counter adversary actions and create positions of relative advantage for US Commanders within the IE, and ultimately the OE.

Notes

1. Preliminary research for this study was conducted in Agarwal et. al., 2017. Since its publication, the research has been updated with revisions such as the correlation to large-scale combat operations. This research was funded in part by the US National Science Foundation (IIS-1636933, ACI-1429160, and IIS-1110868), US Office of Naval Research (N00014-10-1-0091, N00014-14-1-0489, N00014-15-P-1187, N00014-16-1-2016, N00014-16-1-2412, N00014-17-1-2605, N00014-17-1-2675), US Air Force Research Lab, US Army Research Office (W911NF-16-1-0189), US Defense Advanced Research Projects Agency (W31P4Q-17-C-0059), and the Jerry L. Maulden/Entergy Endowment at the University of Arkansas at Little Rock. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organizations. The researchers gratefully acknowledge the support.

2. Department of the Army, Field Manual (FM) 3-13, *Information Operations* (Washington, DC: 2016), 3-3.

3. FM-3-13, 8-25.

4. News BBC, "Russia Fears Crimea Water Shortage as Supply Drops," *BBC News*, 25 April 2014, accessed 12 June 2018, http://www.bbc.com/news/world-europe-27155885.

5. Nitin Agarwal, Samer Al-khateeb, Rick Galeano, and Rebecca Goolsby, "Examining the Use of Botnets and their Evolution in Propaganda Dissemination," *Journal of NATO Defence Strategic Communications* 2, 2017, 87–112.

6. Tuja Khaund, Richard Young, Samer Al-khateeb, and Nitin Agarwal, "Blog Farm Detection Using Social Network Analysis and Social Cyber Forensics Informed Methodologies," in proceedings of the Advances in Social Network Analysis and Mining (ASONAM 2018), 28–31 August 2018, Spain.

7. Alex Cheng and Mark Evans, "Inside Twitter An In-Depth Look at the 5% of Most Active Users," Sysomos Inc., 2009, accessed 12 June 2018, http://sysomos.com/insidetwitter/mostactiveusers.

8. Daisy Sindelar, "The Kremlin's Troll Army: Moscow Is Financing Legions of pro-Russia Internet Commenters. But How Much Do They Matter?" *The Atlantic*, 12 August 2014, accessed 15 June 2018, https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/.

9. Alexel Pavlishak, "Water Supply Problem in Crimea to Cost $247–417 Million - Kremlin Aide," *TASS Russian News Agency*, 28 April 2014, accessed 12 June 2018, http://tass.com/russia/729854.

10. RT News, "Ukraine Builds Dam Cutting off Crimea Water Supply," News Website, RT Question More, (10 May 2014), accessed 12 June 2018, https://www.rt.com/news/158028-ukraine-water-supply-crimea/.

11. Neil Macfarguhar, "Aid Elusive, Crimea Farms Face Hurdles," *The New York Times*, 7 July 2014, accessed 12 June 2018, https://www.nytimes.com/2014/07/08/world/europe/aid-elusive-crimea-farms-face-hurdles.html.

12. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: 2017), 1-5.

13. Quora, "Are You In A Social Media Echo Chamber? How to Take An Objective Look," *Forbes*, 28 February 2018, accessed 20 May 2018, https://www.forbes.com/sites/quora/2018/02/28/are-you-in-a-social-media-echo-chamber-how-to-take-an-objective-look/#718fb21961f9.

14. Shamanth Kumar et al., "TweetTracker: An Analysis Tool for Humanitarian and Disaster Relief," *ICWSM*, 2011, accessed 12 June 2018, http://tweettracker.fulton.asu.edu/Kumar-etal_TweetTracker.pdf; Marc A. Smith et al., "Analyzing (Social Media) Networks with NodeXL," Proceedings of the Fourth International Conference on Communities and Technologies, ACM, 2009, 255–264, accessed 12 June 2018, http://dl.acm.org/citation.cfm?id=1556497.

15. "Conceptual: Deception - GlobalSecurity.org," accessed 28 March 2018, https://www.globalsecurity.org/military/library/report/call/call_3-88_concept.htm.

16. M. Girvan and M.E.J. Newman, "Community Structure in Social and Biological Networks," Proceedings of the National Academy of Science of the United States of America 99, no. 12, 6 April 2002, 7821–26, accessed 12 June 2018, doi:10.1073/pnas.122653799.

17. Department of the Army, FM 3-0, 1-13.

18. Girvan and Newman, "Community Structure in Social and Biological Networks," 7821–26.

19. The term "real person" is used so as not to disclose the identity of this node; Saptarshi Ghosh et al., "Understanding and Combating Link Farming in the Twitter Social Network," Proceedings of the 21st International Conference on World Wide Web, ACM, 2012, 61–70, accessed 12 June 2018, http://dl.acm.org/citation.cfm?id=2187846.

20. Nitin Agarwal, et al. *Journal of NATO Defence Strategic Communications*, 87-112.

Chapter 11

Future Large-Scale Combat Operations (LSCO) Implications for Information Operations

Major General James J. Mingus and Colonel Chris N. Reichart

> *The far-reaching impact of social media, the expansion of information technology, the widespread availability of wireless communications, and competitor influence campaigns have dramatically affected military operations and changed the character of modem warfare.*[1]
>
> —Patrick M. Shanahan, Deputy Secretary of Defense

Over the past 15 years, the Army has focused the majority of its efforts on operations in Afghanistan and Iraq, honing the ability to conduct counterinsurgency operations where information operations efforts were focused more on affecting a non-military population than on enemy decision makers. With the designation of information as a joint function, the Department of Defense has increased the importance of the use of information during operations across the range of military operations, to include during large-scale combat operations. As the military scans the horizon for the character of future conflicts during an era that is increasing being defined by the proliferation and expansion of information-related technologies, information will have a larger—if not decisive—role in the accomplishment of military missions, both in competition and conflict.

The unique aspect of the use of information during military activities is that its effects are potentially global in nature—blurring the lines between the tactical, operational, and strategic levels of conflict. The military can employ the use of information to affect outcomes not only on adversary military formations, but multiple audiences simultaneously, affecting state actors, societies, and individuals not just in the geographical theater of conflict, but globally. In the future, war will be characterized by an increasing use of information and its associated technologies to achieve objectives below the level of armed conflict. Multiple actors, to include nation states, global corporations, transnational terrorists and criminal organizations, societies, and even individuals will all have an important and direct role in the composition and conduct of future conflict. These current and emerging characteristics will require future Army forces to leverage information and associated technologies to understand operational envi-

ronments and employ capabilities to achieve informational effects across multiple systems and audiences to achieve military objectives.

Future adversaries will increasingly look to expand on this global perspective of the information environment, by leveraging expanding informational means to shape and exploit societal and political vulnerabilities on the home-fronts of America and its allies to increase friction amongst friendly actors and undermine and erode strategic resolve. From a defensive standpoint, this dynamic presents a very real and increasing risk to America and its allies that are beholden to maintaining the sanctity of the relationships within the Clauswitzian Triad (e.g. the people, the government, and the military). Indeed, it is a very distinct possibility that a nation state could be strategically defeated during the competition period through the sufficient corruption of these relationships.

While this volume is focused on large-scale combat operations, the use of information has and will continue to have universal application in the accomplishment of positive military outcomes at all echelons. The Army's purpose is to fight and win the nation's wars, but future wars will be multi-domain endeavors that will increasingly stress, and ultimately render useless, traditional operational approaches, paradigms, and processes. Wars of the future will be fought in an increasingly contested information environment, where state and non-state actors will proliferate information through the use of technology on a scale never before seen. The US military will be simultaneously and continuously shaping, preventing, and consolidating gains against adversaries at home and abroad in the information environment to gain and maintain operational and strategic advantage. The future force must account for the use of information across the range of military operations in each of the four Army strategic roles. Information and its employment to achieve military objectives will continue to grow in importance as our adversaries achieve political and military objectives over time below the level of armed conflict.

While the requirement to integrate information-related capabilities to affect adversary decision making is rooted in all military operations, the primary focus for employment of information during past 15 years of counterinsurgency has largely been a population-centric—not adversarial—effort. However, during large-scale combat operations, the Army will need to refocus its efforts to employ these capabilities against enemy information and command and control systems to create conditions in the information environment that place our forces at a position of relative advantage.

The use of current and emerging technology to manipulate information will allow military forces to create false perceptions in the minds of adversary decision makers, causing them to act in a manner that places their forces in a position of relative disadvantage. During modern and future operations, however, commanders must be cognizant of the totality of the information available to adversary decision-making processes. This presents both risk and opportunity. The increasing prevalence of internet-based technologies, to include social media, provide military organizations information that can support or discount efforts to manipulate decision making systems and processes.

In an increasingly interconnected world, future military planners must sufficiently account for efforts to shape a broader information environment, inclusive of social media, the internet, mass media, and artificial intelligence. The internet has allowed information to be disseminated faster, across greater distances, and at greater volumes than at any point in human history. Quite simply, the sheer volume of information available to relevant actors surpasses the capability and capacity of human analysts. This trend will continue to increase exponentially. Technological tools and capabilities will be required in increasing numbers to augment the limits of human analytic abilities and decision making. Machine learning and artificial intelligence that can process big data and automate the observe, orient, decide, act (OODA) loop to operate at inhuman speeds offer glimpses of what this future may look like.

The Army must adapt its culture and processes to elevate the importance of information in future competition and conflict. Current efforts to create an information warfighting function as well as creating an information center of excellence that will develop, produce, and deliver improved capability to operate in the information environment are only the first steps in this effort. However, these efforts alone will have no effect unless the culture of the Army changes. The Army and its leaders must place a premium on the use of information and information technology by devoting the proper resources to change the Army culture. Culturally, Army leaders need to evolve from the narrow approach of massing lethal fires to defeat an enemy army to a more blended approach that combines the massing of lethal and information effects to comprehensively defeat a nation state both militarily and politically. This effort starts in Training and Doctrine Command (TRADOC) at the proponent level, but also requires changes in policy to allow commanders the freedom to employ information and technology from the tactical edge to the operational level.

The Army must initiate change at every echelon across the operating force, and within the generating force, to ensure future commanders have the capability and capacity along with the requisite knowledge and authority to optimally employ information through current and future technologies. Army leaders must account for information and its effects in the operations process, not as a separate effort managed by a separate group of individuals, but mastered by commanders and staffs with the same degree of proficiency by which they employ and maneuver physical forces. Information operators must be just that, operators, capable of integrating physical and informational power seamlessly, as part of operations, and must understand the effects information will have on military formations and civilian entities alike. All operations must be designed with an informational end state and operations, actions, and investments must support that end state. Information capabilities must be inherent in every formation, from tactical to strategic.

The current system of augmentation and reach back capability is insufficient for future conflict. The fact that the majority of the Army's current information forces that would be needed to support LSCO contingencies reside in the reserve component underscores the point that current force structure does not meet projected LSCO force requirements. The Army must balance the requirement for large physical forces with tailored, adaptable information forces that can achieve strategic objectives below the level of conflict through the weaponized use of information.

The US Army is at a pivotal crossroads on how it will employ information power in the future. It can decide to continue on the same path that relegates the use of information to a small group of professionals that have to fight for their relevance on a daily basis, or it can decide to take another course. The US Army can decide to create a total Army force trained, organized, and resourced to operate and prevail in the information environment during the Army's four strategic roles of shape operational environments, prevent conflict, conduct large-scale ground combat, and consolidate gains to achieve outcomes. The US Army can design and approve a strategy to approach operations in the information environment, shaped by policy that provides funding and that concisely assigns roles and responsibilities to achieve Army, Department of Defense, and national objectives. The US Army can align agencies, commands, formations, and proponents that design, build, and deliver capability to the warfighter to achieve information dominance in the conduct of unified land operations. The US Army can develop and elevate a professional, multi-disciplinary capability of generalists and experts that possess the necessary knowledge,

skills, and abilities who are armed with the tools required to deliver operational advantage in the information environment. Only by doing so can the Army provide commanders the information capability and capacity required to gain a position of relative advantage over the enemy not only in the information environment, but also in the operational environment.

This volume, though intended for Army leaders at every echelon, will undoubtedly be read and studied by our allies and adversaries alike. They, too, will glean lessons from this volume—not only on how the Army has used information in the past but seek to learn how the Army will leverage it in the future. For the intended audience, the only question remains is this, "Who will better harness the power of information to defeat an adversary before the battle ensues?" Advantage in the future information environment will start with armies that are culturally inclined to recognizing the potentially decisive nature of information in the "Information Age." Secondarily, achieving informational advantage on the LSCO battlefield will require a professional force that is trained, organized, resourced, and most importantly empowered by commanders to leverage effects efficiently and effectively in the information environment. Will the US Army realize that vision before it is too late?

Notes

1. Memorandum from Deputy Secretary of Defense, "Designated Senior Official for the Integration of Strategic Information Operations and Cyber-enabled Information Operations," 24 May 2018.

About the Authors

Nitin Agarwal

Nitin Agarwal, PhD, is the Jerry L. Maulden-Entergy Endowed Chair and Distinguished Professor of Information Science at the University of Arkansas and Director of the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS). He researches cyber information campaigns, social computing, deviant behavior modeling, group dynamics, social-cyber forensics, data mining, and privacy.

Samer Al-Khateeb

Samer Al-Khateeb, PhD, is an assistant professor in the Department of Journalism, Media, and Computing at Creighton University and a former Postdoctorate Research Fellow at the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS) at the University of Arkansas at Little Rock. His research interests include deviant behavioral modeling; deviant cyber flash mobs; cyber propaganda campaigns; bots behaviors, evolution, and detection; and social cyber forensics.

Lionel M. Beehner

Lionel M. Beehner, PhD, is an assistant professor at the Department of Defense & Strategic Studies at the United States Military Academy at West Point and director of research of West Point's Modern War Institute. He previously was a senior writer at the Council on Foreign Relations. He holds a doctorate in political science from Yale University and a master's of international affairs from Columbia University. His research has appeared in *Security Studies*, *Military Review*, *Parameters*, *Democracy & Security*, *Orbis, Foreign Affairs, The New Republic*, and *The National Interest,* among other publications.

Carmine Cicalese

Colonel (Retired) Carmine Cicalese served for 29 years of active duty in a variety of signal, information operations, and cyberspace operations positions at every headquarter level from platoon to Headquarters, Department of the Army. He was the 1st Cavalry Division IO officer from 2000–03 and 2005–08, with a stint at Joint Special Operations Command from 2003–05. During his first assignment with 1st Cavalry Division, he fulfilled a one-year WIAS tasker that included an assignment to Command Forces Land Component Command (CFLCC). He concluded his information career as Director, Joint Command and Control & Information Op-

erations School and as Division Chief, HQDA G-3/5/7, Cyberspace and Information Operations. Cicalese enjoys sharing his experiences, and especially his failures, with interested information professionals.

Liam S. Collins

Colonel Liam S. Collins is the director of the Modern War Institute at West Point. A career Special Forces officer, he has conducted multiple combat deployments to Afghanistan and Iraq; operational deployments to Bosnia, Africa, and South America; and more than a dozen trips to Ukraine during the 18 months prior to this publication. He has a master's degree and a doctorate from Princeton University.

Dorothy E. Denning

Dorothy E. Denning is Emeritus Distinguished Professor of Defense Analysis at the Naval Postgraduate School. She is author of I*nformation Warfare and Security, Cryptography, and Data Security* and more than 200 articles on topics relating to cybersecurity and cyber conflict. She previously worked at Georgetown University and served as president of the International Association for Cryptologic Research. She has received numerous awards for her pioneering work in cyber security and was inducted into the inaugural class of the National Cyber Security Hall of Fame in 2012. She received BA and MA degrees in mathematics from the University of Michigan and a PhD degree in computer science from Purdue University.

Katrin Galeano

Katrin Galeano is a PhD student at the University of Arkansas. She is majoring in computers and information science and has a research interest in support of the US Army operations security program, in which she volunteers as a social media administrator. Her background is in strategic communications for non-profit and government organizations.

Rick A. Galeano

Lieutenant Colonel Rick A. Galeano is an active-duty US Army officer. He is a PhD student at the University of Arkansas, pursuing a degree in Computers and Information Science. His research interests revolve around strategic communications, social network analysis, and social cyber forensics.

Justin B. Gorkowski

Major Justin B. Gorkowski is a PhD student at the University of Virginia, where he is studying international relations. Prior to this assignment, Gorkowski was a Congressional Fellow in the US Senate and Congressio-

nal Budget Liaison for HQDA. Gorkowski is an information operations officer and previously managed the integration of information-related capabilities in Kandahar, Afghanistan, and Vilseck, Germany for the 2nd Cavalry Regiment.

Robert M. Hill

Robert M. Hill is a military analyst and doctrine writer for the US Army Information Operations Proponent and a retired field artillery and public affairs officer. Over the past decade, he has contributed articles to *Joint Force Quarterly and Military Review* on topics ranging from communication to leadership and women in the Army. He is also a published novelist. He has an MA in English from Duke University and an EdD from the University of Missouri.

Michael E. Kitchens

Michael E. Kitchens is a Department of the Army Civilian as a Doctrine and Concept Developer for the US Army Knowledge Management Office at the Force Modernization Proponent Center (FMPC). He has a master's in Information Management from Webster and undergraduate degrees in Economics and History from Auburn University. Kitchens served on active duty in the US Navy and 28 years in the Army National Guard and Reserve. His military training includes Military Intelligence Basic and Advanced, CAS3, CGSC, Combat Advisor Course, Knowledge Manager Qualification Course and FA-30 Qualification Course (information operations). He served in multiple assignments to include S-2, Information Operations Combat Advisor, Division Knowledge Manager and Division G-7. His most recent assignment before retirement in 2018 was Chief Knowledge Officer (CKO) for US Army Reserve Command, Fort Bragg, North Carolina. He deployed to Operation Iraqi Freedom, Operation Enduring Freedom, and Hurricane Katrina support.

Bradley S. Loudon

Lieutenant Colonel Bradley S. Loudon has been Director of the United States Army Information Operations Qualification Course at Fort Leavenworth, Kansas, since September 2017. Previously as 1st ID's IO Officer, he oversaw Combined Joint Forces Land Component Command-Operation Inherent Resolve's IO efforts in support of large-scale combat operations during the Battle of Mosul (November 2016 to July 2017). Previously, Loudon was selected as the 2014 military recipient of the Secretary of the Army's Pace Award for his work as a HQDA G-3/5/7 Cyber Planner. He has a bachelor's degree in History from the University of Kansas and a Juris Doctorate from Washburn University School of Law.

Christopher W. Lowe

Colonel Christopher W. Lowe has more than 22 years of military service, with more than a decade of experience as an information operations officer. He has master's degrees in Military Arts and Sciences from the US Army School of Advanced Military Studies and in National Resource Strategy from the Eisenhower School, National Defense University.

James J. Mingus

Major General James J. Mingus is the Commanding General of the 82nd Airborne Division. Prior to this assignment, he was the Director, Mission Command Center of Excellence at Fort Leavenworth, Kansas. He commanded at every echelon from company to division, gaining extensive experience with integrating information operations into the operational process during numerous combat deployments. He has a bachelor of science degree from Winona State University and a master's in strategic studies from the US Army War College.

Robert T. Person

Robert T. Person is an associate professor of International Relations at the US Military Academy, where he also serves as Director of Curriculum for West Point's International Affairs Program. He has a PhD in political science from Yale University as well as a master's degree in Russian, East European, and Eurasian Studies from Stanford University. His research focuses on Russian foreign policy and grand strategy, post-Soviet political and economic transitions, Eurasian security, and nationalism in the post-Soviet space. He has conducted extensive field research across Russia, Ukraine, Belarus, the Baltics, the Caucasus, and Central Asia. Person is also a member of the Council on Foreign Relations and a Resident Fellow at West Point's Modern War Institute.

Christopher N. Reichart

Colonel Christopher N. Reichart is the Director of the Force Modernization Proponent Center at Fort Leavenworth, Kansas. He has served as an infantry officer and information operations officer over the past 24 years, recently serving on the CENTCOM staff as the director of several IO portfolios. Reichart holds a Bachelor of Science Degree from the United States Military Academy, a Master of Arts Degree in International Public Policy from the Johns Hopkins School of Advanced International Studies,and a Master of Strategic Studies from the US Army War College.

Brandon S. Riley

Sergeant First Class Brandon S. Riley is a Military Analyst at the Army's Information Operations Proponent at Fort Leavenworth, Kansas. He has a Bachelor of Science in Business Administration from Post University. Riley has served with 1st Cavalry Division, US Army Recruiting Command, 3rd Infantry Division, the US Army Armor School, and the 101st Airborne Division. He has served in leadership positions from Team Leader to Platoon Sergeant and has four operational deployments—two each to Afghanistan and Iraq.

Michael R. Taylor Jr.

Colonel Michael R. Taylor Jr. is an information operations officer. He serves as the Chief, CJ39 Information Operations, for Headquarters Resolute Support, in Kabul, Afghanistan. He has a master's in International Public Policy from the Johns Hopkins University School of Advanced International Studies (SAIS), Washington, D.C.

James N. Turner

Lieutenant Colonel James N. Turner is an active-duty US Army officer. Turner has served for nine years as an information operations planner at the brigade, division, and theater Army level and has honed his understanding during three deployments and multiple training exercises. Turner is respected as one of the most experienced information operations officers at Third Army.

Mark D. Vertuli

Colonel Mark D. Vertuli is the Chief, Operations Plans (J35) for US Strategic Command (USSTRATCOM). He has more than 23 years of military experience and has planned information operations in Afghanistan and the European Command (EUCOM) and Pacific Command (PACOM) areas of operation. He was the battalion commander for 1st Battalion, 1st IO Command (Land) from 2012–14. He has master's degrees in History from Vanderbilt University and in National Resource Strategy from the Eisenhower School, National Defense University.

Andrew D. Whiskeyman

Lieutenant Colonel Andrew D. Whiskeyman is Acting Deputy for the US Central Command (USCENTCOM) Joint Cyber Center. He has more than 23 years of military experience and has worked extensively in the information operations field while deployed to Iraq and Afghanistan. He

earned a doctor of Philosophy in Military Strategy from Air University in 2015 and has master's degrees both from Air Command and Staff College (ACSC) and from the School of Advanced Air and Space Studies (SAASS). He is also a member of the Military Writer's Guild.

Wesley P. White

Wesley P. White is a Department of the Army Civilian. He previously was a sergeant in the 781st Military Intelligence Battalion (Cyber) as a 17C, Cyber Operations Specialist. He has a master's degree in history from the University of Florida, where he wrote his thesis on Chernobyl and its representation in the contemporary Soviet press. During his enlisted career, he was an Exploitation Analyst on a National Mission Team, a job which he continues in his position as an Army Civilian.

Matthew J. Yandura

Colonel Matthew J. Yandura is Chief, Concepts, Requirements, Integration, Personnel, and Doctrine for the Information Operations Proponent at Fort Leavenworth, Kansas. He has a Bachelor of Applied Arts in Interpersonal-Public Communication from Central Michigan University and a master's in International Relations from The Catholic University of America. He has served with the XVIII Airborne Corps, 82nd Airborne Division, 173rd Airborne Brigade Combat Team, 11th Psychological Operations Battalion, US Army Cadet Command, US Military Training Mission to Saudi Arabia, and the US Security Coordinator for Israel and the Palestinian Authority. He has served in leadership positions from Platoon Leader to Chair and Professor of Military Science at Loyola University-Chicago. Yandura has three combat and two operational deployments to Afghanistan, Iraq, Saudi Arabia, Kuwait, and Israel respectively.

U.S. Army Combined Arms Center