

Broadening Traditional Domains

Commercial Satellites
and National Security

Ulysses S. Grant and
the U.S. Navy



Joint Force Quarterly

Founded in 1993 • Vol. 97, 2nd Quarter 2020
<https://ndupress.ndu.edu>

GEN Mark A. Milley, USA, Publisher
VADM Frederick J. Roegge, USN, President, NDU

Editor in Chief
Col William T. Eliason, USAF (Ret.), Ph.D.

Executive Editor
Jeffrey D. Smotherman, Ph.D.

Production Editor
John J. Church, D.M.A.

Internet Publications Editor
Joanna E. Seich

Copyeditor
Andrea L. Connell

Associate Editor
Jack Godwin, Ph.D.

Book Review Editor
Brett Swaney

Art Director
Marco Marchegiani, U.S. Government Publishing Office

Advisory Committee

Ambassador Erica Barks-Ruggles/*College of International Security Affairs*; RDML Shoshana S. Chatfield, USN/U.S. Naval War College; Col Thomas J. Gordon, USMC/*Marine Corps Command and Staff College*; MG Lewis G. Irwin, USAR/*Joint Forces Staff College*; MG John S. Kem, USA/U.S. Army War College; Cassandra C. Lewis, Ph.D./*College of Information and Cyberspace*; LTG Michael D. Lundy, USA/U.S. Army Command and General Staff College; LtGen Daniel J. O'Donohue, USMC/*The Joint Staff*; Brig Gen Evan L. Pettus, USAF/*Air Command and Staff College*; RDML Cedric E. Pringle, USN/*National War College*; Brig Gen Kyle W. Robinson, USAF/*Dwight D. Eisenhower School for National Security and Resource Strategy*; Brig Gen Jeremy T. Sloane, USAF/*Air War College*; Col Blair J. Sokol, USMC/*Marine Corps War College*; Lt Gen Glen D. VanHerck, USAF/*The Joint Staff*

Editorial Board

Richard K. Betts/*Columbia University*; Eliot A. Cohen/*The Johns Hopkins University*; Richard L. DiNardo/*Marine Corps Command and Staff College*; Aaron L. Friedberg/*Princeton University*; Bryon Greenwald/*Joint Forces Staff College*; COL James E. Hayes, USA/*National War College*; Douglas N. Hime/*Naval War College*; Col Jerome M. Lynes, USMC (Ret.)/*The Joint Staff*; Kathleen Mahoney-Norris/*Air Command and Staff College*; Bert B. Tussing/*U.S. Army War College*

Cover 2 images (top to bottom): Marines conduct demolition breaching tactics during exercise Bougainville II on Range 9, Pohakuloa Training Area, Hawaii, May 12, 2019 (U.S. Marine Corps/Jacob Wilson); Paratrooper assigned to 4th Infantry Brigade Combat Team (Airborne), 25th Infantry Division, participates in joint forcible entry exercise at Joint Base Elmendorf-Richardson, Alaska, August 23, 2016 (U.S. Air Force/Javier Alvarez); Airmen assigned to Team Eglin take Polar Bear Plunge into Choctawhatchee Bay, January 18, 2019, at Eglin Air Force Base, Florida (U.S. Air Force/Samuel King, Jr.)



In This Issue

Forum

- 2 Executive Summary
- 4 The Imperative for the U.S. Military to Develop a Counter-UAS Strategy
By Edward A. Guelfi, Buddhika Jayamaha, and Travis Robison
- 13 The Challenge of Dis-Integrating A2/AD Zone: How Emerging Technologies Are Shifting the Balance Back to the Defense
By Alex Vershinin
- 20 Proliferated Commercial Satellite Constellations: Implications for National Security
By Matthew A. Hallex and Travis S. Cottom
- 30 Electronic Warfare in the Suwalki Gap: Facing the Russian "Accompli Attack"
By Jan E. Kallberg, Stephen S. Hamilton, and Matthew G. Sherburne

JPME Today

- 39 Strategic Leader Research: Answering the Call
By Larry D. Miller and Laura A. Wackwitz
- 47 Expanding Atrocity Prevention Education for Rising U.S. National Security Leaders
By David Wigmore
- 55 The Missing Element in Crafting National Strategy: A Theory of Success
By Frank G. Hoffman

Commentary

- 65 The Joint Force Needs a Global Engagement Cycle
By Gregory M. Tomlin
- 73 Detention Operations as a Strategic Consideration
By John F. Hussey

Features

- 83 Transforming DOD for Agile Multidomain Command and Control
By Douglas O. Creviston



About the Cover

Army women's team and Marines men's team each came in first during joint quarterly running competition known as Commander's Cup, held at Presidio's Soldier Field, on July 21, 2017, with the Marine Corps Detachment Presidio of Monterey claiming Commander's Cup for best combined time, Presidio of Monterey, California (U.S. Army/ Steven Shepard)

- 91 Disciplined Lethality: Expanding Competition with Iran in an Age of Nation-State Rivalries
By Scott J. Harr
- 97 Countering A2/AD in the Indo-Pacific: A Potential Change for the Army and Joint Force
By Hassan M. Kamara

Recall

- 103 Learning the Art of Joint Operations: Ulysses S. Grant and the U.S. Navy
By Harry Laver

Book Reviews

- 110 Boy on the Bridge
Reviewed by Bryon Greenwald
- 111 To Build a Better World
Reviewed by Walter M. Hudson
- 112 The Russian Understanding of War
Reviewed by Maria Y. Omelicheva

Joint Doctrine

- 114 Airbase Defense Falls Between the Cracks
By Joseph T. Buontempo and Joseph E. Ringer
- 121 Putting the "FIL" into "DIME": Growing Joint Understanding of the Instruments of Power
By Cesar Augusto Rodriguez, Timothy Charles Walton, and Hyong Chu

- 128 Update

Joint Force Quarterly is published by the National Defense University Press for the Chairman of the Joint Chiefs of Staff. *JFQ* is the Chairman's flagship joint military and security studies journal designed to inform members of the U.S. Armed Forces, allies, and other partners on joint and integrated operations; national security policy and strategy; efforts to combat terrorism; homeland security; and developments in training and joint professional military education to transform America's military and security apparatus to meet tomorrow's challenges better while protecting freedom today. All published articles have been vetted through a peer-review process and cleared by the Defense Office of Prepublication and Security Review.

NDU Press is the National Defense University's cross-component, professional military and academic publishing house.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government.

Copyright Notice

This is the official U.S. Department of Defense edition of *Joint Force Quarterly*. Any copyrighted portions of this journal may not be reproduced or extracted without permission of the copyright proprietors. *JFQ* should be acknowledged whenever material is quoted from or based on its content.

Submissions and Communications

JFQ welcomes submission of scholarly, independent research from members of the Armed Forces, security policymakers and shapers, defense analysts, academic specialists, and civilians from the United States and abroad. Submit articles for consideration to ScholarOne, available at <https://mc04.manuscriptcentral.com/ndupress>, or write to:

Editor, *Joint Force Quarterly*

NDU Press
300 Fifth Avenue (Building 62, Suite 212)
Fort Lesley J. McNair
Washington, DC 20319
Telephone: (202) 685-4220/DSN 325
Email: JFQ1@ndu.edu
JFQ online: ndupress.ndu.edu/jfq

2nd Quarter, April 2020
ISSN 1070-0692



Army Project Manager Tactical Network works to find solutions that enable larger numbers of smaller satellites to orbit closer to Earth, April 11, 2019 (Courtesy International Space Station)

Executive Summary

In the inaugural issue of *Joint Force Quarterly*, space was a part of the discussion when then-Air Force Chief of Staff General Merrill McPeak wrote his “Ideas Count” article. General McPeak stated, “I believe the Air Force should consolidate all U.S. military operations in space.” A generation later, we have picked up on his suggestion. The joint force has expanded at the strategic and operational levels in a historic move to

create a new combatant command: the United States Space Command. The new command will give this initiative its tactical workforce once the details are finalized. What will it mean to the joint force and to joint warfighting? I suspect a great deal after the administrative actions are worked out.

In the past decade, we have seen the addition of the National Guard to the Joint Chiefs of Staff, and now the

Chief of Space Operations joins them as a new Service chief. While General Jay Raymond, U.S. Space Force, will have the smallest force at the table and report to the Secretary of the Air Force, as Air Force Chief of Staff General David Goldfein does, his team has arguably the biggest domain to work in. For the joint force, U.S. Space Command has returned to the combatant commanders’ table in its second life, having first appeared

from 1985 to 2002. In addition, General Raymond will be dual-hatted as U.S. Space Command's commander.

To readers of *JFQ*, space as a warfighting domain—or the desire to have a separate Service—is not a new idea. However, the idea of a separate Service is one that had to overcome a great deal of opposition and bureaucratic inertia. Will this separation allow for a better focus on this warfighting domain? Will acquisition decisionmaking and management of space programs be better? The most important issues that have arisen in recent years should be at the top of the operations and planning staffs' agendas. How to better “control” space in ways that might be useful to the other concepts of domain control; what responsibilities the force will have in space; and what the tactical, operational, and strategic relationships will be between space warfighters and their counterparts are just a few of the issues. A persistent problem will be the still-unresolved issue of how to allocate airpower to the land component commander’s preferences when other domains compete for those limited assets. And the international treaty obligations for space cannot be ignored without affecting our relations with other space-faring nations as well. We look forward to seeing how U.S. Space Force and U.S. Space Command develop.

In the Forum, we offer a variety of discussions that center on the emerging technologies of today and tomorrow’s battlespace. As a recent briefing by a U.S. commander engaged in the fight against the so-called Islamic State acknowledged, our defenses against unmanned aircraft systems are limited and deserve attention, especially around our fixed infrastructure and bases in forward areas. Edward Guelfi, Buddhika Jayamaha, and Travis Robison discuss the immediate requirement for the development of a strategy to counter these threats. Equally prominent in security debates has been the antiaccess/area-denial (A2/AD) challenges to our joint force. Alex Vershinin posits that technology is shifting the advantage back to defense. And as reports of more than 50,000 satellites will be in orbit in the coming years, Matthew

Hallex and Travis Cottom discuss how the rapid increase in commercial satellites will affect our national security. Another important, yet sometimes neglected, issue is electronic warfare. *JFQ* alumnus Jan Kallberg, Stephen Hamilton, and Matthew Sherburne discuss how to identify advances in Russian capabilities that the joint force needs to counter.

In JPME Today, Larry Miller and Laura Wackwitz discuss how to conduct research to support the education of strategic leadership in our staff and war colleges. With the 75th anniversary of the liberation of the Nazi death camps fresh in our minds, David Wigmore provides us with a solid roadmap on how to educate our future national security leaders to prevent atrocities in the future battlespace. Frank Hoffman returns to *JFQ* with his views on the missing part of our national strategy—a theory for success. After nearly two decades of war with seemingly no obvious prospect of victory in a classic sense, his ideas cannot be more welcomed.

Gregory Tomlin leads off our Commentary section by suggesting that the development of a global engagement cycle is critical to the success of global integration. In addition, having recently served as the Deputy Commander at Guantánamo Bay detention camp, John Hussey reviews the history and lessons to be learned from detainee operations.

In Features, Douglas Creviston discusses the urgent need to change and adapt the joint force command and control structure through a transformation of the Defense Department. Scott Harr, in an article written before the recent killing of Iranian General Qasem Soleimani, offers insights on how lethality can be an important part of dealing with Iran as a rival nation-state. Hassan Kamara discusses how the U.S. Army and the joint force can address A2/AD threats in the U.S. Indo-Pacific Command region.

Harry Laver, in our Recall article, takes us back to the Civil War to see how General Ulysses S. Grant and Andrew Foote, a naval officer, learned to work together successfully. We also bring you three excellent book reviews that will help

you learn about a range of important joint and strategic issues.

This issue’s Joint Doctrine section offers two important articles that speak directly to the seams in joint operations, instruments of power, and the pursuit of strategy’s ends. As reliance on using forward-deployed airpower to back up local forces in combat operations grows, one question Joseph Buontempo and Joseph Ringer address is who will provide airbase defense. And in an effort to raise awareness within the joint force of the financial, intelligence, and law enforcement aspects of how we employ the instruments of national power to fulfill national security strategy, Cesar Rodriguez, Timothy Walton, and Hyong Chu suggest that only looking at diplomatic, informational, military, and economic options often lead to less than optimal strategic results. Finally, with many important changes to Joint Doctrine coming every month, all of them can be tracked in our update.

JFQ has been involved in the discussion of space since our inception in 1993. The debates on how best to be joint, fight joint, and help our partners integrate with us has been our bread and butter from the start. I look forward to an increased discussion on the way ahead for the joint force on land, sea, air, space, cyberspace, and anywhere else our freedoms need defending. *JFQ*

WILLIAM T. ELIASON
Editor in Chief



Soldier pushes RQ-7B Shadow unmanned aerial system on Joint Base McGuire-Dix-Lakehurst, New Jersey, February 2020 (U.S. Air National Guard/Matt Hecht)

The Imperative for the U.S. Military to Develop a Counter-UAS Strategy

By Edward A. Guelfi, Buddhika Jayamaha, and Travis Robison

Major Edward A. Guelfi, USA, is an Executive Officer at the 2nd Battalion, 11th Field Artillery Regiment. Dr. Buddhika Jayamaha is a Faculty Member at the United States Air Force Academy. Lieutenant Colonel Travis Robison, USA, is a Battalion Commander at the 2nd Battalion, 11th Field Artillery Regiment.

Military power often emerges at the nexus of technology, organizational processes of force employment, and training.¹ However, rapid technological change, the constantly evolving character of warfare, and the lingering effects of sustained combat on military readiness constrain

the U.S. military's ability to respond to emerging global security challenges. The proliferation of unmanned aerial systems (UAS), more commonly referred to as drones, represents one of the largest emerging challenges to the joint community since the rise of improvised explosive devices during the onset of Operation *Iraqi Freedom*. Recent conflicts involving state and nonstate actors and the acquisition priorities of U.S. rivals like Russia and China demonstrate that Soldiers on future battlefields will see the widespread use of drones. For example, Russia and Russian-backed separatists have used various types of drones to achieve devastating effects during their ongoing conflict with Ukraine.² U.S. forces in Syria could not retain operational control of the airspace below 3,500 feet for an extended period of time where the so-called Islamic State (IS) conducted lethal and nonlethal drone operations.³ Looking ahead, the

Department of Defense (DOD) anticipates that China will soon outspend the United States in drone investment, with more than \$10 billion dedicated solely to research and development, and may become the world leader in this area by 2023.⁴

For the first time in more than six decades, U.S. ground forces have found themselves under aerial attack and are generally unable to counter the threat. Existing air defense systems have proved tragically unable to detect or engage slow, low-flying UAS.⁵ Failure to mitigate this operational risk across the full spectrum of conflict will leave the U.S. Army vulnerable to the use of drones by state and nonstate adversaries. This risk results in an imperative for the Army to develop and implement a more comprehensive counter-UAS strategy than currently exists and that must include material, organizational, and Soldier solutions. Drones present a multidomain challenge, so improving the Army's counter-UAS strategy will provide a framework for developing and integrating counter-UAS capabilities into emerging warfighting concepts. This article explains the UAS threat in terms of technological diffusion and patterns of use and provides counter-UAS recommendations for consideration by senior military leaders.

The Threat

Technological Diffusion. The Cold War demand for persistent surveillance of the Soviet Union led the Air Force and U.S. intelligence agencies to pursue UAS development by the late 1950s, and these drone technologies materialized in the early 1960s.⁶ During the latter part of the 1960s, the United States employed these new technologies to monitor China's development of nuclear and air defense capabilities, as well as to conduct battle damage assessments during the Vietnam War.⁷ Following that conflict, the United States struggled to integrate UAS into its European operations against the Soviet Union due to technological and airspace restrictions.⁸ Regardless, the United States continued to improve drone technologies and by the 1990s had successfully developed the Predator, which

provided operationally viable persistent surveillance capabilities.⁹

The first operational deployment of a Predator squadron occurred in Bosnia in 1995, where it provided targeting information, monitored refugee flows, and provided battle damage assessments.¹⁰ After seeing the operational benefits of 24-hour persistent surveillance in rough terrain and adverse weather conditions, Congress more than doubled the Predator budget and accelerated additional UAS programs, which subsequently became the foundation of current global drone fleets and tactics.¹¹ While the United States initiated the use of UAS, over the past two decades drones have proliferated throughout the world. Today, more than 90 state and nonstate actors possess drone capabilities ranging from small, commercial drones to more sophisticated military variants. Moreover, at least 16 countries have armed drone programs with another 20 countries attempting to develop them.¹² The evolution of electronics and software technologies and the changing character of warfare converged to influence the rapid and widespread proliferation of civilian and military drones. Today, there are more than 600 types of armed and unarmed drones used or being developed around the world.¹³

The accessibility, affordability, and capabilities of available UAS influence their proliferation. Small, affordable, and commercially available hobbyist drones are less capable overall, but they provide groups with an accessible intelligence, surveillance, and reconnaissance (ISR) capability that often rivals more sophisticated military variants. For example, the Chinese-made DJI Mavic is a commercially available quadcopter that costs less than \$100 and is capable of autonomous takeoffs and landings, flying GPS-programmed routes, tracking and following moving objects, and sensing and avoiding obstacles.¹⁴ The Mavic's degree of autonomous flight currently exceeds that of the U.S. Air Force's approximately \$17 million MQ-9 Reaper UAS.¹⁵

Israel is currently the largest exporter of military UAS, with over 60 percent of international transfers over the past

30 years.¹⁶ But between 2010 and 2014, only approximately 2.5 percent of transferred drones were armed, so the majority of UAS transferred abroad have been unarmed systems primarily intended for reconnaissance.¹⁷ The number of armed drone exports is increasing, however, given the number of countries actively developing UAS. In particular, China is quickly becoming a leader in exporting inexpensive, weapons-capable drones.¹⁸

Commercial UAS are proliferating more rapidly than military variants because of the latter's higher cost and greater support infrastructure requirements, as well as existing international arms trade agreements.¹⁹ The availability and proliferation of commercial systems throughout the security environment complicate military responses because these drones often have comparable capabilities to small military UAS and can be easily modified for military uses.²⁰ Next-generation commercial drone technology is making these systems more like military ones, and they are exploiting new operational concepts such as swarming.²¹ As a result, as UAS technology continues to advance and proliferate, the distinctions between commercial and military drones will become less clear, further enhancing operational risk.

As drone proliferation continues, military leaders must understand the capabilities and limitations of each type of drone to develop effective countermeasures. Currently, DOD classifies drones into one of five categories based on a system's size, speed, and operational range.²² While helpful in distinguishing between a system's potential use in tactical or operational roles, these categories do not provide a roadmap for understanding two important UAS characteristics as they relate to likely battlefield use: a system's degree of accessibility or availability, and the technology and infrastructure required to support using a system. These two characteristics result in a taxonomy of UAS with four categories: hobbyist drones, midsize military and commercial drones, large military-specific drones, and stealth combat drones.²³ Each category of drones has distinct capabilities and limitations that provide a foundation for determining how to counter a system.

Hobbyist drones are widely available for purchase by the public and generally cost less than \$3,000. These systems come preassembled or may require assembly; however, they do not require training to operate or any support infrastructure. Midsize military and commercial drones are generally unavailable because of their cost and infrastructure requirements. However, these systems are often sold or transferred by states to foreign militaries and nonstate actors. Large military-specific UAS include reconnaissance and armed variants and are rarely operated by actors other than major militaries because of the systems' costs and infrastructure requirements. Stealth combat drones contain highly sophisticated technologies such as jamming resistance and low observability and are only accessible to those states that produce the systems. Currently, the United States is the only known operator of stealth UAS; however, several countries are developing stealth combat drones.²⁴

Patterns of Use. Drones are becoming more sophisticated and capable of conducting surveillance to lethal attacks, either as a delivery system or as an inexpensive precision-guided weapon. The ongoing pursuit and development of artificial intelligence and swarming ability suggest a future where numerous small and inexpensive systems might be used to achieve localized overmatch against a more capable force such as the U.S. Army.²⁵ The proliferation, sophistication, and weaponization of commercially available UAS mean that any state or nonstate actor will have access to this technology and will likely employ it in novel ways. Moreover, the use of drones may be strategically ambiguous because the international perception of the use of UAS in crises or conflicts is quite different than the use of traditionally piloted aircraft in similar circumstances.²⁶

Wider use of drones may reshape military operational concepts and how states engage in conflict. The strategic ambiguity inherent in these systems increases the military options available to an actor, particularly in gray zone conflict or similar contested environments where multiple parties might claim control over

airspace. Drones can lower the risks of certain actions such as violating another state's airspace because these systems operate without placing a human pilot at risk. But the lack of a human pilot also lowers the risk of a state using force against a drone during an incursion. Recent examples of this dynamic occurred in 2014 when Turkey shot down a suspected Russian UAS, and in 2015 when Syria reportedly shot down a U.S. Predator, neither of which resulted in escalation or retaliation.²⁷ For nonstate actors, drones may provide a military capability they otherwise would not have.²⁸ For instance, Russian-backed Ukrainian separatists have used drones to spot artillery strikes.²⁹ Another example occurred in 2016 and 2017, when IS launched air attacks against Iraqi troops using small armed drones.³⁰

The level of tactical and operational risk to U.S. ground forces has increased dramatically, as more than 23 countries, including Russia, China, Iran, and North Korea, are known to possess or in the process of developing armed drone capabilities.³¹ The list of hostile nonstate actors with drone capabilities is also rapidly growing and now includes terrorist organizations such as IS, Hizballah, and Hamas and insurgent groups such as Houthi rebels in Yemen.³² In Africa, Boko Haram recently started employing armed drones in cross-border attacks on Nigeria and Cameroon.³³ Lastly, given al Shabaab's ties with Hizballah, it is likely only a matter of time before the group begins using drones in support of its terror operations.³⁴

Russia, China, and Iran have armed drone capabilities, and these states have demonstrated operational innovation in the employment of small tactical drones. The behavior of these states in recent conflicts highlights how the use of drones increases the complexity of modern conflict, the effects of operational innovations and proliferation, and how a near-peer competitor might seek to exploit current U.S. military vulnerabilities. Together, Russia, China, and Iran's behaviors and capabilities highlight what the U.S. Army must expect from adversaries in every region of potential conflict.³⁵

Russia rapidly implemented a drone development and acquisition program that entailed purchasing Israeli-made UAS while concurrently investing in domestic sourcing programs.³⁶ During its incursion into Crimea and Eastern Ukraine in 2014—the latter instance widely believed to be the first in which every belligerent used drones to produce decisive battlefield results—Russia and its proxies used tactical drones to provide ISR targeting information for supporting artillery units. The near real-time intelligence from these small platforms improved target location accuracy, counterfire response times, and fire mission lethality,³⁷ and in one instance in July 2014, Russia used this technique to destroy four Ukrainian army brigades preparing to conduct a cross-border attack against Russian-backed separatists' lines of supply.³⁸

Whereas Russia demonstrates innovation in drone tactics, Iran displays an inclination toward technical innovation. Iran started its drone program decades ago during its conflict with Iraq, and it is now one of the most developed in the Middle East.³⁹ Iran has also demonstrated its willingness to share advanced drone technology with others throughout the region. It reportedly flew drones such as the Shahed-129 over Iraq and Syria, exported drone technology to Hizballah and Hamas, and may have provided an assortment of drones to Houthis in Yemen and shared advanced drone technology with Russia.⁴⁰ The U.S. military has also engaged and destroyed two Iranian-made drones in Syria that conducted an attack against U.S. ground forces. Incidents such as these highlight that Iran is continuing to expand its drone programs and is willing to employ drones as an asymmetric counter to U.S. military superiority. Iranian drones have been reported in locations from Pakistan to Syria and throughout the Persian Gulf region. They have also become the centerpiece of Iranian technology exhibits used to showcase their advanced security capabilities despite rigorous international sanctions.⁴¹

The extent of China's UAS development in support of its military remains unclear to Western military analysts and



Soldiers from 7th Air Defense Artillery Regiment engage targets with Patriot missile systems at NATO Missile Firing Installation at Chania, Greece, during German-led multinational air defense exercise Artemis Strike, November 2017 (U.S. Army/Jason Epperson)

senior leaders; however, there is evidence that China's efforts are a real cause for concern. Some experts believe that the Chinese military's drone efforts focus on swarming technology, increased payload and operational range, and the incorporation of artificial intelligence. In a congressionally mandated report, analysts noted that the number and types of China's domestically developed unmanned aerial vehicles continue to expand, with five new platforms displayed at the 2016 Zhuhai airshow.⁴² China also appears to be betting that swarms of low-tech drones linked with high-tech artificial intelligence will become the weapon of choice in future conflicts and capable of countering any military force, including that of the United States. China's level of effort in developing UAS suggests the importance and relevance it perceives the technology holds for potential future conflict.⁴³

Besides the activities of rival states, the recent employment of drones by nonstate

actors reveals how quickly and relatively easily these groups can disrupt advanced industrial militaries. Drones are attractive to these groups because of “the way they carry [destructive] power and the distance from which they allow an adversary to control its delivery.”⁴⁴ Small commercially available drones give groups such as IS the ability to field an air force capable of collecting ISR and providing limited close air support. The evolution of non-state actors’ use of small drones began in 2004 when Hezbollah used drones to challenge the Israeli military.⁴⁵ Drone use by nonstate groups continues to evolve and demonstrates the ability to conduct complex attacks. For instance, during the year-long fight to recapture Mosul, Iraqi security forces faced persistent armed drone attacks that slowed their efforts to liberate IS-held neighborhoods.⁴⁶ Of concern is the increasingly complex and disruptive ways in which nonstate actors use tactical drones. Hezbollah uses these systems for surveillance, manufacturing

propaganda, armed strike missions, and kamikaze-type attacks.⁴⁷ The Russian ministry of defense recently reported that in January 2018, its forces in western Syria experienced an attack by a “swarm of home-made drones.” According to the ministry, Russian forces at Khmeimim Air Base and Tartus naval facility faced a complex attack by 13 drones armed with small-diameter bombs that caused casualties and damaged facilities.⁴⁸ These types of swarm-like attacks are particularly threatening because existing kinetic defenses struggle to cope with the agility of small drones, and swarming would overwhelm most existing countermeasures.⁴⁹

Recommendations for Counteracting the Threat

U.S. policy must not only respond to today’s problems, but it should also be flexible enough to adapt to tomorrow’s challenges. A comprehensive counter-UAS strategy must address the different nature of threats presented by

the various types of UAS. It must also provide solutions for confronting the full scope of UAS challenges by potential state and nonstate adversaries. The U.S. Army's current counter-UAS strategy does not do this. The discussion herein shows that U.S. adversaries are learning and adapting, but the Army is failing to keep pace. Russia's operational employment of drones in Ukraine, Iran's proliferation of drone technologies, China's emphasis on developing full-spectrum drone capabilities, and the evolution of drone use by nonstate actors show that Army planners must anticipate extensive UAS employment in future conflicts. Changes in drone technologies and evolving adversary doctrines suggest that the Army must learn from recent conflicts, as the Russians did, and recognize that the changing character of warfare requires improved acquisition processes and training to effectively counter the UAS threat.

During the global war on terror, the Army made the deliberate decision based on budget priorities to emphasize long-range air defense systems by significantly reducing and eliminating short-range air defense systems. According to senior leaders, this decision was a calculated risk taken when leaders believed that the current and future capabilities of the Air Force would defeat any aerial threat and maintain air superiority.⁵⁰ As the assumptions underlying this decision have been proved invalid, the elimination of short-range air defense systems means the Army now relies on aging antiaircraft and missile intercept systems to counter every UAS threat.⁵¹ Given the proliferation of tactical drones, the use of advanced air and missile defense systems is inappropriate due to cost, system availability, and an inability to defeat slow, low-flying drones.

Recently, the Israel Defense Forces employed their U.S.-made Patriot missiles against a single small drone from Syria that violated Israeli airspace. The Israelis used multiple \$3 million PAC-2 missiles but failed to destroy the target.⁵² This incident highlights the unsustainable cost and technical difficulty of employing limited theater-level air defense assets against tactical drones.⁵³ In 2017,

then-commanding general of the U.S. Army Training and Doctrine Command, General David Perkins, told an audience, "If I'm the enemy, I'm thinking, 'Hey, I'm just going to get on eBay and buy as many of these \$300 quadcopters as I can and expend all the Patriot missiles out there.'"⁵⁴ If the Patriot and Stinger missiles—which cost \$3 million and \$38,000 each, respectively—remain the primary defense means for countering drones, it may be possible for an adversary to employ tactics such as those IS used against Russia in Syria to deplete a theater-level air defense capacity that costs tens of millions of dollars. This low-cost act would make an entire area of operations vulnerable to subsequent air attack.

Though the U.S. Army has taken steps to improve its counter-UAS capabilities, these actions have been insufficient. The Army recently began the process of expanding the availability of short-range air defense systems in the Active force by having its Materiel Command overhaul legacy Avenger systems previously set to be destroyed. Though a step in the right direction, reintroducing short-range air defense systems will take time, during which maneuver forces will remain vulnerable. The Army took additional steps to mitigate this gap by training and assigning Stinger teams to its maneuver forces, along with developing Stinger upgrades to improve their effectiveness against tactical drones.⁵⁵ However, this is a solution that has already been proved ineffective. When the Army made a similar attempt to integrate Stinger teams in the 1990s, senior defense officials noted that the result "was not great, as we found that 80 percent, if not more, of all Stinger shots taken by maneuver Soldiers, were done in a revenge fashion, after the enemy had already destroyed most of the formation."⁵⁶ As the drone threat continues to evolve, so too must the solutions used to counter the threat.

The current drone threat is far too complex for a single solution to solve. A U.S. Army counter-UAS strategy must provide a framework for a persistent and comprehensive approach that links Soldier, materiel, and software solutions. The Army must creatively employ all

means along these three lines of effort to regain operational initiative. Along the Soldier line of effort, the Army must retrain its troops to compete, fight, and win in a drone-saturated environment and to win in the counter-reconnaissance fight while restructuring its formations to meet the added demands of counter-drone requirements. Along the materiel solutions line, the Army must continue its reforms of an industrial age—acquisition process to promote rapid, creative, and independent technical solutions through public-private partnerships with corporate partners. Lastly, the Army must explore existing and emerging commercial technologies to identify counter-UAS measures it can rapidly field along with innovative software solutions compatible with existing systems. If no such technologies exist, the Army will have to spearhead the development of effective counter-UAS systems. The newly created U.S. Army Futures Command, whose mission is intended to result in a more rapid acquisition process, can spearhead these efforts. Early success in this command along these lines might provide an opportunity for the Army to leap ahead in drone technology and in ways to counter the drone threat.⁵⁷

The Army must place its primary emphasis on the Soldier line of effort, since this is arguably the most important in terms of near-term counter-UAS effectiveness. This requires redeveloping atrophied air defense warfighting skills necessary in a contested drone environment. Capability and training in air defense skills declined during decades operating in uncontested airspace and counterinsurgency operations. The Army previously trained Soldiers in the fieldcraft necessary to conduct active and passive air defense. Active measures include tasks involving the detection and engagement of enemy aircraft; passive defense measures include skills related to camouflage, concealment, position hardening, dispersion, and mobility to guard against air attack.⁵⁸ To its credit, the Army is starting to reintroduce training related to these skillsets.⁵⁹

Reintroducing and strictly enforcing standards of the passive defense is a low-cost and rapid solution to



Explosive ordnance disposal technician flies DJI Mavic Pro Drone while forward deployed in Middle East, May 2017 (U.S. Marine Corps/Shellie Hall)

immediately counter enemy drone threats. If Ukrainian forces at Zelenopillya in July 2014 had implemented passive air defense measures, the results of the Russian attack likely would have been much less severe. The Army should invest in home-station training kits of commercial drone systems like it did following the emergence of the improvised explosive device threat in the battlefields of Iraq and Afghanistan. Once the Army realized the magnitude of the threat posed by these devices, it quickly integrated methods designed to train deploying units in how to counter and defeat the threat. The Service also tested preparedness during culminating training events at its three combat centers. The same approach must be applied to counter-UAS training.

The arrival and detection of any enemy UAS can no longer be considered a mere inconvenience to the detected formation but immediately elevated to the commander's attention, as that origination

must actively engage the threat while breaking contact to ensure its survival. The kinetic options to engage an enemy UAS once detected vary from the simple to the complex, but what has proved most effective to date often merges both the traditional kinetic and emerging nonkinetic options to achieve a layering of joint effect against the UAS platform. It is with this approach that all following suggestions should be considered. No single line of effort will be enough to defeat or even suppress this threat alone. It will require the layering of all of these efforts for the U.S. Army and the joint force to achieve a desirable outcome in this new counter-reconnaissance fight.

The blurred distinction between commercial and military drone production makes it necessary for the Army to study and understand the future potential of these systems by working with commercial industry partners. Given the current reliance of nonstate actors on the commercial development of this technology,

collaborating with major manufacturers, including foreign manufacturers, will offer the Army insights on the direction of system change and potential threats. This early understanding will provide time for the Army to develop appropriate responses before adversaries employ the systems on the battlefield. As the Under Secretary of the Army recently announced regarding the creation of Army Futures Command, “We have to get more agile in how we work with both of those key constituencies or communities.” He also noted that the “entire Department of Defense really divested a lot of its systems engineering talent back in the 1990s and it’s been a challenge for the department for weapon systems development because of not having that organic capability inside the department.”⁶⁰

Army Futures Command is the ideal organization to implement the search for and development of materiel solutions to counter drones. The Army must ensure



Tim Giles pilots drone during ThunderDrone Tech Expo at SOFWERX in Tampa, Florida, September 2017 (U.S. Air Force/Barry Loo)

that the command is properly manned and given the necessary authorizations to become an institution that can reform an acquisition system that has become unable to keep pace with modern technological change. The U.S. Special Operations Command's relationship with SOFWERX provides a model for what larger scale Army materiel collaboration might look like. SOFWERX is a public-private technology incubator that has recently been preparing to host a series of drone competitions to explore how these systems and equipment might benefit the command.⁶¹ This public-private model would benefit the larger conventional Army and provide a venue to not only discover how drones might benefit the Service but also devise ways to counter them.

While global reach on commercial drone systems is still an emerging technology, the areas that will have significant impacts on a commercial-to-military crossover remain steadily focused on improvements in autonomous flight,

increased battery performance, and location technologies. Currently, there remain few commercial drones that can fly without the aid of a user-directed path, but this technology is quickly emerging along with the application of commercial artificial intelligence. Advances in location technologies will also present a significant challenge to the military. The stated goal of companies working in this area is to build systems that can identify their location without the aid of GPS.⁶² Combining all the above technological advancements into a single commercial platform—and there is little reason to suspect that will not happen—will provide a potential adversary a commercial version of the most advanced military drones in the world. The Army must work with industry partners that could provide it with forewarning of when this may occur and perhaps influence the timing.

The final line of effort for developing a counter-UAS strategy is to link Soldier and materiel solutions with systems

software within the existing structure of Army brigade combat team systems. The first step in formulating these solutions will require developing software for existing systems that enable detecting and tracking drones. Current air tracking systems are already capable of tracking larger operational drones, so the focus must be on smaller tactical UAS, which have smaller radar cross sections due to their small infrared and electromagnetic signatures. Therefore, the Army must invest in software for current and future sensors that can better detect tactical drones. The uncertain budget environment makes the acquisition of new radar systems unlikely, and previous acquisition failures suggest that the Army should not invest limited funds in a specialized counter-drone radar. Instead, it must develop better software for existing radars like the AN/MPQ-64 Sentinel and AN/TPQ-53 radar systems. The latter system was originally designed to track rocket, artillery, and mortar rounds, but the Army is testing its ability

to track drones. One advantage that modern radars have is active electronically scanned arrays.⁶³ Radars with this feature have proved more versatile than older systems, so developing software for these systems to track tactical drones provides a solution short of developing a new radar system.

General Mark A. Milley believes, “One of our most important duties as [military] professionals is to think clearly about the problem of future armed conflict.” He also notes that fixed sites of any kind will be lethal magnets for destruction by enemies who will have a rich diet of targeting information.⁶⁴ This information will likely be provided in large part by hostile drones, some of which might conduct attacks. Recent conflicts involving state and nonstate actors and the drone acquisition priorities of U.S. rivals seem to confirm this reality. Despite these threats and the observable lessons from recent conflicts, the Army remains vulnerable to the long-term operational risks resulting from the proliferation and use of drones by state and nonstate adversaries. The reemergence of long-term geopolitical competition with rivals employing a variety of drones, rapid diffusion of drone technologies throughout every operational region, and adversary warfighting concepts that integrate drones into effective offensive operations result in a strategic imperative for the Army to develop and implement a counter-UAS strategy based on Soldier, materiel, and software solutions. This type of strategy will provide a framework for improving the Army’s acquisition process to better leverage emerging technologies and develop a comprehensive Soldier training program that integrates these technologies to regain the initiative through improved warfighting. The Army has spent trillions of dollars in the last decade building and generating a force that can fight, dominate, and win in the land domain, yet states and groups with far fewer resources are rising to challenge the United States in the new arena of drone warfare. The Army must take all necessary steps to mitigate this threat or risk losing the next war. JFQ

Notes

¹ Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2006).

² Phillip A. Karber, “Lessons Learned” from the Russo-Ukrainian War: Personal Observations,” draft, Johns Hopkins Applied Physics Laboratory and U.S. Army Capabilities Center, July 2015, 12, available at <<https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf>>.

³ Mark Pomerleau, “How \$650 Drones Are Creating Problems in Iraq and Syria,” *C4ISRNET*, January 2018, available at <www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/>.

⁴ Ian McPhedran, “U.S. Predicts 42,000 Unmanned Chinese Military Planes by 2023,” News Corp Australia Network, July 8, 2015, available at <www.news.com.au/world/asia/us-predicts-42000-unmanned-chinese-military-planes-by-2023/news-story/b9b5bc-52967c7347cb977f9b3460f98f>.

⁵ Pomerleau, “How \$650 Drones Are Creating Problems in Iraq and Syria.”

⁶ Thomas P. Ehrhard, *Air Force UAVs: The Secret History* (Arlington, VA: Air Force Association, July 2010).

⁷ Drones conducted 93 percent of damage assessments following Operation *Linebacker II*. See also Ehrhard, *Air Force UAVs*, 9, 28.

⁸ Ehrhard, *Air Force UAVs*, 32–33.

⁹ Frank Strickland, “An Insider’s Perspective on Innovation During Fiscal Austerity: The Early Evolution of the Predator Drone,” *Strategies in Intelligence* 57, no. 1 (March 2013), 6; Richard Whittle, *Predator: The Secret Origins of the Drone Revolution* (New York: Henry Holt & Co., 2014).

¹⁰ Arthur Holland Michel, “Drones in Bosnia,” Center for the Study of the Drone, Bard College, New York, June 7, 2013, available at <<http://dronecenter.bard.edu/drones-in-bosnia/>>; Elizabeth Becker, “Crisis in the Balkans: The Drones; They’re Unmanned, They Fly Low, and They Get the Picture,” *New York Times*, June 3, 1999, available at <www.nytimes.com/1999/06/03/world/crisis-balkans-drones-they-re-unmanned-they-fly-low-they-get-picture.html>.

¹¹ Michel, “Drones in Bosnia”; Strickland, “An Insider’s Perspective on Innovation During Fiscal Austerity,” 3.

¹² Matt Fuhrmann and Michael C. Horowitz, “Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles,” *International Organization* 71, no. 2 (Spring 2017), 397–418.

¹³ Lynn E. Davis et al., *Armed and Dangerous? UAVs and U.S. Security* (Santa Monica, CA: RAND, 2014), 7–10; *United States Army Counter-Unmanned Aircraft System (C-UAS) Strategy Extract* (Washington, DC: Army Capabilities Integration Center, 2016), 5.

¹⁴ More information on the DJI Mavic can be found at Web site of SZ DJI Technology Co., Ltd., available at <www.dji.com/mavic-air?site=brandsite&from=nav>.

¹⁵ James Drew, “USAF to Automate MQ-9 Takeoffs and Landings,” *Flight Global*, May 4, 2016, available at <www.flighthglobal.com/news/articles/usaf-to-automate-mq-9-takeoffs-and-landings-424975/>.

¹⁶ George Arnett, “The Numbers Behind the Worldwide Trade in Drones,” *The Guardian*, March 16, 2015, available at <www.theguardian.com/news/datablog/2015/mar/16/numbers-behind-worldwide-trade-in-drones-uk-israel>.

¹⁷ Ibid.

¹⁸ Kyle Mizokami, “For the First Time, Chinese UAVs Are Flying and Fighting in the Middle East,” *Popular Mechanics*, December 22, 2015, available at <www.popularmechanics.com/military/weapons/news/a18677/chinese-drones-are-flying-and-fighting-in-the-middle-east/>.

¹⁹ Andrea Gilli and Mauro Gilli, “The Diffusion of Drone Warfare? Industrial, Organizational, and Infrastructural Constraints,” *Security Studies* 25, no. 1 (February 2016), 50–84.

²⁰ Ben Watson, “The Drones of ISIS,” *Defense One*, January 12, 2017, available at <www.defenseone.com/technology/2017/01/drones-isis/134542/>; Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, “Separating Fact from Fiction in the Debate over Drone Proliferation,” *International Security* 41, no. 2 (Fall 2016), 7–42.

²¹ Alexis C. Madrigal, “Drone Swarms Are Going to Be Terrifying and Hard to Stop,” *The Atlantic*, March 7, 2018, available at <www.theatlantic.com/technology/archive/2018/03/drone-swarms-are-going-to-be-terrifying/555005/>.

²² Micro-tactical, small tactical, tactical, persistent, penetrating. See *Unmanned Systems Integrated Roadmap FY 2013–2038* (Washington, DC: Department of Defense, 2014), available at <<http://apps.dtic.mil/cgi-bin/fulltext/u2/a592015.pdf>>.

²³ Kelley Sayler, *A World of Proliferated Drones: A Technology Primer* (Washington, DC: Center for a New American Security, June 2015), 8, available at <<http://drones.cnas.org/reports/what-are-drones/>>.

²⁴ For details on the capabilities, limitations, and technological trends of these four categories of drones, see *ibid.*

²⁵ Ibid.

²⁶ Michael C. Horowitz, Paul Scharre, and Ben FitzGerald, *Drone Proliferation and the Use of Force: An Experimental Approach* (Washington, DC: Center for a New American Security, March 2017), available at <<http://drones.cnas.org/reports/drone-proliferation-use-force/>>.

²⁷ Orhan Coskun, “Turkey Shoots Down Drone Near Syria, U.S. Suspects Russian Origin,” *Reuters*, October 16, 2015,

available at <www.reuters.com/article/us-mideast-crisis-turkey-warplane-idUSKCN0SA15K20151016>; Missy Ryan, "U.S. Drone Believed Shot Down in Syria Ventured into New Area, Official Says," *Washington Post*, March 19, 2015.

²⁸ Horowitz, Kreps, and Fuhrmann, "Separating Fact from Fiction in the Debate over Drone Proliferation," 7–42.

²⁹ Sydney Freedberg, Jr., "Russian Drone Threat: Army Seeks Ukraine Lessons," *Breaking Defense*, October 14, 2015, available at <<http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/>>.

³⁰ Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat from ISIS: Exploding Drones," *New York Times*, October 11, 2016, available at <www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>; Watson, "The Drones of ISIS."

³¹ Davis et al., *Armed and Dangerous?* 9.

³² Peter Bergen, Melissa Salyk-Virk, and David Sterman, *World of Drones* (Washington, DC: New America Foundation, November 22, 2019), 4, available at <www.newamerica.org/in-depth/world-of-drones/3-who-has-what-countries-armed-drones/>.

³³ Simon Ateba, "Boko Haram Terrorists Now Using Drones in Nigeria and Cameroon," *The Nigerian Voice*, September 4, 2017, available at <www.thenigerianvoice.com/news/256790/boko-haram-terrorists-now-using-drones-in-nigeria-and-cameroon.html>.

³⁴ "Nigerian Army Links Boko Haram to Hezbollah," *Sahara Reporters*, May 30, 2013, available at <<http://saharareporters.com/2013/05/30/nigerian-army-links-boko-haram-hezbollah>>.

³⁵ Karber, "'Lessons Learned' from the Russo-Ukrainian War," 12.

³⁶ Nicholas Clayton, "How Russia and Georgia's Little War Started a Drone Arms Race," *PRI*, October 23, 2012, available at <www.pri.org/stories/2012-10-23/how-russia-and-georgia-s-little-war-started-drone-arms-race>.

³⁷ Karber, "'Lessons Learned' from the Russo-Ukrainian War," 12.

³⁸ Shawn Woodford, "The Russian Artillery Strike that Spooked the U.S. Army," Mystics & Statistics blog, March 29, 2017, available at <www.dupuyinstitute.org/blog/2017/03/29/the-russian-artillery-strike-that-spooked-the-u-s-army/>.

³⁹ Ariane Tabatabai, "Iranian Drone Program," *Bulletin of the Atomic Scientists*, October 12, 2017, available at <<https://thebulletin.org/decades-making-iranian-drone-program11185>>.

⁴⁰ Levi Maxey, "Next-Gen Drones: Making War Easier for Dictators and Terrorists," *The Cipher Brief*, December 12, 2017, available at <www.thecipherbrief.com/next-gen-drones-making-war-easier-dicta>.

tors-terrorists>; John Kester, "Russian Drone Tech May Include Help from Iran," *Foreign Policy*, October 5, 2017, available at <<http://foreignpolicy.com/2017/10/05/russian-drone-tech-may-include-help-from-iran/>>.

⁴¹ "U.S. Shoots Down Second Iran-Made Armed Drone Over Syria in 12 Days," *The Guardian*, June 20, 2017, available at <www.theguardian.com/us-news/2017/jun/20/us-iran-drone-shot-down-syria>.

⁴² According to the *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017* (Washington, DC: Department of Defense, May 15, 2017), 29, "China displayed five airframes: the Wing Loong I, Wing Loong II, WJ-600A/D, Yunying Cloud Shadow, and the CH-5 (Rainbow 5)."

⁴³ Emily Feng and Charles Clove, "Drone Swarms vs. Conventional Arms: China's Military Debate," *Financial Times*, August 2017, available at <www.ft.com/content/302fc14a-66ef-11e7-8526-7b38dcaef614>.

⁴⁴ Brian A. Jackson, *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica, CA: RAND, 2008), xv.

⁴⁵ Avery Plaw and Elizabeth Santoro, "Hezbollah's Drone Program Sets Precedents for Non-State Actors," *Terrorism Monitor* 15, no. 21 (November 10, 2017).

⁴⁶ Jamie Crawford, "Report Warns of ISIS Developing Drones for Chemical Attacks," CNN, October 20, 2016, available at <www.cnn.com/2016/10/20/politics/terrorist-groups-and-drones/index.html>.

⁴⁷ Plaw and Santoro, "Hezbollah's Drone Program Sets Precedents for Non-State Actors."

⁴⁸ David Reid, "A Swarm of Armed Drones Attacked a Russian Military Base in Syria," CNBC, January 11, 2018, available at <www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html>.

⁴⁹ Madrigal, "Drone Swarms Are Going to Be Terrifying and Hard to Stop."

⁵⁰ Randall McIntire, "The Return of Army Short-Range Air Defense in a Changing Environment," *Fires Bulletin* (November–December 2017), 5.

⁵¹ Barry Pike, Program Executive Officer, Missiles and Space, statement, *On Fiscal Year 2018 Priorities and Posture of Missile Defense Programs and Activities: Hearing Before the Subcommittee on Strategic Forces, Committee on Armed Services, United States House of Representatives*, 115th Cong., 8 (2017).

⁵² Callum Paton, "Iran Drone No Match for U.S. Patriot Missile as Israel Blows Hezbollah Aircraft Out of the Sky," *Newsweek*, September 2017, available at <www.newsweek.com/iran-drone-no-match-us-patriot-missile-israel-blows-hezbollah-aircraft-out-sky-667570>.

⁵³ "IDF Fails 3 Times to Bring Down Drone over Golan," *Times of Israel*, July 17,

2016, available at <www.timesofisrael.com/idf-we-tried-and-failed-3-times-to-bring-down-drone-over-golan/>.

⁵⁴ Alexandra Larkin, "How Do You Shoot Down a \$200 Drone? With a \$3 Million Patriot Missile," CNN, March 16, 2017, available at <www.cnn.com/2017/03/16/americas/drone-shot-by-patriot-missile-trnd/index.html>.

⁵⁵ McIntire, "The Return of Army Short-Range Air Defense in a Changing Environment," 5–6.

⁵⁶ Interview with senior Defense official, February 2017.

⁵⁷ Jen Judson, "Army Futures Command Taking Charge of Conjuring Up New Capability," *Defense News*, March 24, 2018, available at <www.defensenews.com/digital-show-dailies/global-force-symposium/2018/03/24/army-futures-command-taking-charge-of-conjuring-up-new-capability/>.

⁵⁸ Christopher L. Spillman and Glenn A. Henke, "The New Threat: Air and Missile Defense for Brigade Combat Teams," *AUSA Magazine*, February 17, 2017.

⁵⁹ Anne Chapman, *The National Training Center Matures, 1985–1993* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 1997), 26.

⁶⁰ Judson, "Army Futures Command Taking Charge of Conjuring Up New Capability."

⁶¹ Michael Bottoms, "SOFWERX: A Smart Factory of Innovation Helping the Warfighter," U.S. Special Operations Command Office of Communication, February 2, 2018, available at <www.socom.mil/pages/SOFWERX—A-smart-factory-of-innovation-helping-the-warfighter.aspx>.

⁶² Judson, "Army Futures Command Taking Charge of Conjuring Up New Capability."

⁶³ Sydney J. Freedberg, Jr., "Drone Defense: Army Anti-Artillery Radar Tracks UAVs," *Breaking Defense*, June 27, 2016, available at <<http://breakingdefense.com/2016/06/drone-defense-army-anti-artillery-radar-tracks-uavs/>>.

⁶⁴ David Barno and Nora Bensahel, "Three Things the Army Chief of Staff Wants You to Know," *War on the Rocks*, May 23, 2017, available at <[www.warontherocks.com/2017/05/three-things-the-army-chief-of-staff-wants-you-to-know/](http://warontherocks.com/2017/05/three-things-the-army-chief-of-staff-wants-you-to-know/)>.



Airman secures Joint Air to Surface Standoff Missiles on flatbed truck at munitions storage area on Ellsworth Air Force Base, South Dakota, October 2019, as part of U.S. Strategic Command's exercise Global Thunder 20 (U.S. Air Force/Christina Bennett)

The Challenge of Dis-Integrating A2/AD Zone

How Emerging Technologies Are Shifting the Balance Back to the Defense

By Alex Vershinin

Today, America's adversaries are building antiaccess/area-denial (A2/AD) zones to keep the U.S. military out of key strategic regions. A2/AD is a series of sensors; antiship, antiaircraft, and ground defenses; and long-range fires utilized by U.S. competitors and designed to prevent the United States from entering into a close fight.¹ We see Chinese A2/AD zones set up to deny U.S. access to Taiwan and the South China Sea. Russia uses A2/AD zones in Kaliningrad, Crimea, the Kola Peninsula, and the Kuril Islands to block key maritime avenues of approach. In the past, the weakness of these zones were the command and control nodes, which formed a

Lieutenant Colonel Alex Vershinin, USA, is Director of Technical Integration at the Army Futures Command Studies Group.

single point of failure. Utilizing precision-guided technology, the United States would wage a short, inexpensive decapitation campaign aimed at these nodes. Their destruction would break up integration of enemy defenses, also called *dis-integration*. For decades, the offense-defense balance was firmly on the offense. Emerging technologies in the fields of network, artificial intelligence, and space are shifting the balance back to defense, making these zones more dangerous. At the same time, the United States may have overestimated the effects of long-range strike capabilities after three decades of fighting non-peer competitors. Unable to fight a short decapitation campaign, the United States may be forced into a prolonged attrition campaign, at unacceptable political costs.

What Is A2/AD?

A2/AD zones are composed of intelligence, surveillance, reconnaissance (ISR), and defensive and offensive strike systems. ISR systems are utilized to spot incoming threats for engagement by defensive strike systems. Offensive strike systems attack enemy bases, logistics, and command and control (C2) infrastructure seeking to delay the buildup of U.S. forces. Adding to the effectiveness of the A2/AD zones are the decoy and deception operations that favor ground-based defenders and increase the defender's survivability. Combinations of these techniques with emerging technologies are making defense the stronger form of warfare for the foreseeable future. The key strategic objective of the defender is not to defeat the United States in battle, but to increase the costs to the United States until the potential political gain is outweighed by the loss.

Current: Advantage Offense (United States)

Traditionally, the defender has relied on combinations of ground-based radars, human intelligence, and ground reconnaissance to gain an operational picture. Wealthier states could afford to augment these sensors with an Airborne

Warning and Control System (AWACS), consisting of powerful radars mounted on large passenger planes, unmanned aerial vehicles, and space assets. The augmenting assets are expensive and available only in small numbers. This makes them early high-value targets, unlikely to survive prolonged conflict. Within a month of conflict, the United States would destroy most of them, forcing the defender to rely on his primary systems for early warning and targeting.

For the U.S. military, the main strike capability has always been land- and sea-based airpower. U.S. adversaries' solutions were ground-based air defense. These air defenses are relying on ground-based search radar to identify incoming strikes and attack radar, which paints the targets for the defending missile. The search radar has numerous weaknesses. It is stationary; thus, its coverage is limited and can be bypassed. Once turned on, electronic warfare (EW) aircraft can identify its location and destroy it with standoff antiradiation missiles that home in on radar emissions. Historically, an attacking air force can suppress air defenses after a month-long air campaign.² Ground search radars can be augmented with AWACS. These aircraft are more survivable than ground-based radars due to their mobility, but the introduction of long-range and very long-range air-to-air missiles, together with low observable aircraft, are rapidly negating the effects of AWACS, retaining advantage for offense.

Reliance on ground-based search radar forces the defender to centralize the C2 structure. Passing targeting data between batteries requires a single central control node. This weakness is exacerbated by the effectiveness of suppression of enemy air defense missions using anti-radiation missiles. Unable to continuously emit, defenders must rely on rolling emissions by several radars to gain a picture of their airspace. It is a process where several radars cover the same area and turn on and off for short durations before moving. Only a centralized headquarters can coordinate that effort and tie it in with defending fighters. This gives the attacker few key nodes for targeting. Destruction

of these nodes will rapidly dis-integrate the enemy's A2/AD defense. The missile launchers will still be there, but they will not be able to engage without warning and targeting data telling them where to shoot. So far, the balance is in favor of the offense.

Next 10 Years: Advantage Defense (Adversary)

Emerging technologies are changing this 10-year prediction. One key technology is the miniaturization of cameras and satellites. New microsatellites are cheap, small, and effective. A single rocket can deliver 80 small photo reconnaissance satellites into orbit.³ This technology has allowed the U.S. firm Planet to photograph any corner of the Earth with one of its 200 satellites, updating images every day with 2-meter resolution.⁴ The defender does not need to cover all the Earth; he just needs to cover the conflict zone. He can accomplish this by seeding the orbit over the conflict zone with 300 to 500 microsatellites, especially if these satellites are able to generate imagery of 1-meter resolution and transmit data every 5 to 10 minutes. This satellite constellation will have complete photo coverage of the battlespace and be able to spot any aircraft or ship coming into the conflict zone. This system is even more dangerous because antisatellite weaponry is extremely expensive. For example, both antiballistic and antisatellite (Standard Missile 3, or SM-3) missiles cost between \$15 and \$18 million each. To make matters worse, in 2018 the Department of Defense planned to buy only 40 of them.⁵ There may simply not be enough antisatellite missiles to destroy an enemy constellation. There are direct energy weapons coming online, and the Russians recently claimed to have operationalized one.⁶ Yet even those systems are few in number and may not be able to attrit a satellite constellation faster than the enemy can reseed it. In short, this constellation may be extremely survivable to the point where an attacker might not be able to neutralize it due to the large number of targets.

Space-based ISR will be augmented by aerostats. These are high-altitude balloons or blimps. They can maintain a position at 70,000 feet above sea level and have visual coverage of up to 775 miles.⁷ Aerostats vary in cost but are far cheaper than interceptor missiles and can be easily replaced. Functionally, they are like microsatellites—a cheap and resilient, wide-area ISR system.

More powerful high-speed computers allow algorithms to rapidly process thousands of surveillance images, identifying incoming aircraft or ships based on pre-programmed image recognition. It also allows prediction of trajectories based on several images collected with the ability to pass that data across the battle network. The United States has been working on a similar capability in Project Maven.⁸ This data will not be enough for targeting, but it will generate an early warning system robust enough to replace ground-based radar systems without any of their weaknesses. As computers get smaller, they can be mounted on the microsatellite. This allows data processing to be done in space and only targeting data to be passed across the network. This reduces the bandwidth requirements and speeds up the time to identify targets. Instead of updating target location every 5 minutes, it can be done every minute, resulting in greatly increased effectiveness of early warning systems.

Where an attacker can gain an advantage is in the defender's logistics. Once enemy air defense artillery fires, it requires resupply. An attacker can use the same space-based ISR combined with high-speed computing power to develop algorithms to track resupply vehicles traveling to locations from which missile launches have been detected. This method will give the attacker a general idea where the enemy defenses are; unfortunately, the defender must start shooting before it can be utilized.

Another defensive advantage is electronic warfare. The increased bandwidth and processing power of computers allow U.S. adversaries to network their electronic reconnaissance. By networking all his EW reconnaissance assets with analytical systems, the defender can analyze



Standard Missile-3 Block 1B interceptor missile launches from USS *Lake Erie* during Missile Defense Agency and U.S. Navy test in mid-Pacific, May 2013 (U.S. Navy)

the emissions of attackers in real time and determine which targets are real and which are decoys. It can rapidly identify incoming threats that generate emissions that may have been missed by other systems. Russia has this capability in its Moskva-1 system.⁹

Underpinning the enemy system is the network. For any data to be relevant, it must be easily passed from one system to another. The network must be robust

and secure. Quantum computing technology introduces communications that are long range, difficult to locate, and nearly impossible to break into.¹⁰ This network allows data to be rapidly passed between early warning satellites and ground-based defense systems. In addition, the defender owns terrain and will have time to lay fiber cable between his battle positions, reducing emissions and defending its network against jamming.

It will be difficult to isolate specific portions of the battlefield. We know that our adversaries are looking to develop such networks and technologies, and it is only a matter of time before they succeed.¹¹

How the New ISR Comes Together

The defender will retain ground-based search radars but keep them off and rely on satellites and aerostats to provide early warning and to cue attack radars. Without emissions by the ground-based radars, the attacker will be unable to locate enemy antiaircraft and antiship missile batteries before they fire. The ground search radars will only be activated if the network fails, giving the A2/AD complex redundancy should it be temporarily dis-integrated. Neutralizing them will become far more time-consuming and costly in terms of munitions expended and aircraft lost. The penetration of a robust A2/AD system requires the attacker to converge complementary capabilities from multiple units and services. The challenge is the amount of time needed to plan such a deliberate operation and the availability of key capabilities. If any capability such as EW aircraft is not available, then the entire mission must be canceled.

The digital network that passes data directly from satellite and aerostat early warning systems to the ground-based shooters allows the defender to decentralize command and control. Data carried across the network is generated by each reconnaissance node and is seen by all shooting nodes. For example, when a satellite constellation picks up a target, it automatically puts the data out on the network so that every shooting battery sees it without headquarters in the loop. Even fighter aircraft can operate independently based on priorities published prior to conflict. This system removes headquarters as a single point of failure in a defender's A2/AD zone, making the task of dis-integrating more challenging. A recent speech by General Valery Gerasimov, chief of the Russian general staff, indicates that this is the direction Russia is planning to go.¹²

Survivability

The next key topic is the survivability of adversary A2/AD systems. There are two issues. The first is the effects that munitions have on targets and the number of strikes needed to fully neutralize enemy defenses. The second is the increased effectiveness of modern decoys and camouflage.

Decreasing Effects of Long-Range Fires

The most common long-range fire systems employed by U.S. forces are Tomahawks and Joint Air-to-Surface Standoff Missile—Extended Range (JASSM-ER) long-range missiles. Their key advantages are their long range (over 1,000 kilometers), precision, and the absence of danger to human pilots. They can be delivered by aircraft, submarines, and surface ships. In the past, these weapons were fired early in a conflict to destroy search radars, degrade airbases, and neutralize key nodes in an enemy's A2/AD system. The effectiveness of these weapons may be overestimated because we have fought non-peer enemies. During the conflict in Syria, the United States employed massive cruise missile strikes on two occasions; in both cases, the damage inflicted was in no way proportional to the amount of munitions used.

During the strike on Shayrat Airbase on April 7, 2017, the United States fired 59 missiles. Satellite imagery shows only 44 targets hit, although some may have been hit twice.¹³ It is possible that Russian jamming may have diverted some missiles off target, although there is no way to be certain without access to classified information. Russia's Krasukha, an electronic warfare jamming system, was reported in the area at the time of the strike.¹⁴ Regardless, the airbase was launching airstrikes less than 24 hours after the attack.¹⁵ While the base was warned an hour ahead of the strike, it was not equipped or postured to endure a conventional precision strike.

The second strike took place on April 14, 2018. A combination of 109 JASSM-ERs, Tomahawks, and SCALPs (a European cruise missile) was fired

at six buildings. The second strike was purely political in nature and is harder to assess for weapon effectiveness. There are indications that some of the incoming missiles (Tomahawks and SCALPs) were intercepted. The Russian government has presented missile remnants showing clear damage from air defense artillery (ADA) fragmentation impacts.¹⁶ In addition, there is video evidence from Damascus showing incoming missiles intercepted by defensive missiles.¹⁷

At sea, the situation has been even more difficult. An attacker's surface ships entering A2/AD zones are vulnerable to antiship missiles, especially new hypersonic systems such as the Chinese DF-26 and Russian Zircons. Even submarine launches are becoming a challenge as defending diesel submarines are becoming quieter and increasing their submerged time thanks to independent air propulsion. During an April 2018 North Atlantic Treaty Organization (NATO) missile strike, a state-of-the-art British *Astute*-class nuclear submarine was located and harassed by a pair of Russian *Kilo*-class diesel submarines. It is suspected that it failed to participate in the attack because of the harassment.¹⁸ The combination of antiship missiles and cheap diesel submarines can be used to keep attacker's ships away from an A2/AD zone. It is possible that in the future, aircraft will be the only means of reliably launching cruise missiles.

The number of missiles required to destroy a target is another issue, and there may not be enough missiles in U.S. inventories. Official reports indicate that approximately 100 to 150 missiles are purchased every year.¹⁹ Quick math shows that missiles introduced in 1983 would result in 4,500 missiles in stock, at 125 missiles purchased for 36 years. About 2,000 have been expended in combat.²⁰ That leaves an inventory of 2,500. At 100 missiles per major target, the U.S. stockpile is empty after 25 targets. Even then, the damage is rapidly repairable as the Shayrat Airbase strike demonstrated. Once the stockpile is depleted, the United States will be reliant on replacing hundreds of Tomahawks and JASSM-ERs a year. As enemy EW

and ADA continue to improve, the required expenditure of missiles per target will only go up. Traditionally, the United States could rely on its industrial base to ramp up prior to conflict. This may not be possible. A recent report by an interagency task force points to a decline in U.S. industrial bases' potential. A decrease of skilled labor, combined with foreign parts in the supply chains, suggest that the United States may not be able to ramp up production prior to conflict. Instead, America may suffer temporary disruption of production.²¹

Once standoff weapons are expended, the attacker will be forced to rely on manned aircraft to penetrate the A2/AD zone. This will immediately drive up the cost—in lives, aircraft, finances, and political capital for the attacker. Manned aircraft can generate far more strikes but are vulnerable to the same ADA as a cruise missile. In addition, there is a human factor. Faced with incoming fire, pilots may choose to drop their munitions and abort. Cruise missiles will press on, no matter the odds.

A2/AD zones are able to soak up tremendous amounts of conventional fire power without long-term effects, especially those of near-peer competitors whose industrial base will replace losses and restore the effectiveness of A2/AD zones after repeated strikes.

One of the best examples of A2/AD zone resilience is the Siege of Malta, which took place from June 1940 to November 1942. The island, sitting in the middle of the Mediterranean Sea, was able to conduct air and sea denial against Axis shipping for the duration of the North African campaign. Despite committing over 2,000 aircraft during the campaign, German and Italian forces failed to neutralize the island for any length of time. When the battle was over, Malta-based forces had sunk 23 percent of total European Axis shipping. The key to the island's defenses was heavy ADA, distribution of aircraft across numerous small airfields, and a constant air patrol. Logistics were distributed across numerous small caches rather than one large supply point. The airfields were rapidly repaired and put back into action. The



USS Monterey fires Tomahawk land attack missile in U.S. Fifth Fleet area of operations, April 2018 (U.S. Navy/Matthew Daniels)

key takeaway from that battle is that most damage inflicted on an A2/AD zone is temporary and will be repaired given even a short respite.²²

Defenders can use many of the same techniques today. Dispersing aircraft across multiple airfields, always keeping a combat air patrol airborne, and using highway segments as runways can serve to make fixed-wing aircraft more survivable and allow them to enhance the A2/AD zone. Strikes at airbases work only if aircraft are on the ground. This system's point of failure is sustainment. Using highway segments increases survivability, but someone must fuel, rearm, and then park the aircraft. Maintenance is a major issue, especially for fifth-generation aircraft. During Operation *Desert Storm*, U.S. F-15s and F-16s generated one sortie a day. In 2018, F-35s generated only 0.33 sorties per day while flying from USS *Essex* against the Taliban.²³ Providing maintenance assets at dispersed locations requires considerable coordination. Although both sides have to contend with long-range fires, the defender has the advantage because he had years to plan and rehearse dispersed operations on familiar terrain.

It is important to note that munition effects cut both ways. There is an assumption that Russian missiles will destroy

NATO infrastructure and prevent use of NATO airbases in range of Russian A2/AD zones. This is highly unlikely. Russian missiles are newer, and the country has not had time to build large stockpiles. As noted above, it takes almost 100 missiles to close an airfield to operations, and the effect is only temporary. The U.S. Air Force adaptive bases concept adds to resilience by further spreading out aviation assets and increasing the Russian target list. The Russians are far more likely to concentrate their limited missile inventory on key targets such as C2 nodes and logistic support areas, including forward fuel storage facilities.

Decoys and Deception

The capacity of the defense is further increased by decoys and deception countermeasures. These can work both ways but usually favor the defender. Decoys are used to absorb fire power and divert from real targets. Attackers can use decoys to mislead a defender and overwhelm the ADA with targets, but with aircraft being the main striking platform, this becomes more difficult. In theory, airborne decoys are possible, but they must fool radar, EW, and the visible spectrum from space-borne ISR assets, all while maneuvering at Mach 2. The price tag of this decoy will rapidly

approach the cost of an actual combat aircraft. Ground systems are much easier to hide using underpasses and vegetation, while ground decoys are cheaper since they can be stationary. The defender has a major advantage when it comes to camouflage and deception operations.

During the 1999 conflict in Kosovo, the Serbian army made extensive use of decoys to absorb NATO airstrikes. According to one report filed by the U.S. Air Force Munitions Effectiveness Assessment Team, 90 percent of reported hits were on decoys. In an extreme case, the Serbs even managed to protect a bridge by constructing a decoy 300 meters downriver. The decoy bridge was designed to be seen from the air and was struck multiple times by NATO aircraft.²⁴ The spoofing did not end in visual range. Serbian air defenses also used extensive radar decoys to divert NATO suppression of enemy air defense missions away from actual radars. Serbian Colonel Zoltán Dani, commander of the 250th Air Defense Missile Brigade, used old radar sets pulled from obsolete fighters to divert NATO strikes away from search and attack radars. During the war, his brigade was engaged more than 20 times with NATO antiradiation missiles without any effect. The decoys absorbed all the damage. Using such innovative techniques, his brigade was credited with shooting down two NATO aircraft, including a stealth F-117, and damaging another.²⁵

The lessons of the Kosovo War were not lost on our adversaries; the Russian army has institutionalized Serbian techniques. While Serbian weaponry was a quarter-century behind, the state-of-the-art A2/AD zones in Russia and China are equipped with modern systems. To provide concealment and deception, the Russian army has created the 45th Engineer-Camouflage Regiment. This formation is tasked with camouflaging targets so they cannot be found and creating dummy targets that divert an attacker's fire power.²⁶ The Russians make extensive use of inflatable decoys. Their dummy tanks can be transported in two duffel bags, resist

minor shrapnel damage, and incorporate radar-reflective coating.²⁷ It is suspected that a battery-powered heater can be used to generate a heat signature. It appears that this technology was tested in Syria with satisfactory effects.²⁸ The regiment not only hides formations; it can also disguise an installation and build a fake airfield in 24 hours.²⁹ In addition to setting up decoys and disguising physical targets, the formation has capabilities to simulate radio and radar emissions for full-spectrum deception operations. When combined with constant shifting of forces around the battlefield such as moving aircraft between airfields and patches of highways, these tools can be highly effective.

Systems deployed by formations such as the 45th regiment are not capable of complete deception, especially against higher end space platforms, but they do not have to be. They are designed to defeat tactical-level collection platforms such as the microsatellite ISR described earlier. The problem with national-level collection platforms is that there are few of them and they are tasked to support national- and strategic-level targets, not tactical operations. The small number leaves them vulnerable to enemy antisatellite systems.

Another technique is to make all systems look alike. The proliferation of standardized containers for international shipping is making the camouflage of weaponry even easier. Recently, both Russia and China have introduced anti-ship missile launchers that are disguised as containers.³⁰ Northrop Grumman has also investigated this technology.³¹ As space-based ISR becomes more resilient and robust, we can expect all vehicles to start looking the same. The attackers will have no way of knowing if the observed truck is carrying a deadly antiship missile or hauling humanitarian supplies to a refugee camp. By making all targets look the same, the defender can degrade the effects of enemy fire power and protect his key defense systems.

A defender's techniques are not all powerful and will not prevent an attacker's penetration of the A2/AD zone. Once key U.S. systems are converged,

penetration of the A2/AD zone is possible. A strike package would consist of EW protection and attack aircraft to jam radars and incoming missiles, cyber attack to disrupt the enemy network, and ground- and sea-based long-range fires to disrupt enemy ADA and airbases, all timed to allow strike aircraft to penetrate the A2/AD zone. A defender's deception operations and the survivability of his formations will degrade the effects that the penetrating strike force has, while attacking platforms are engaged by state-of-the-art air defenses. The attacker will penetrate the A2/AD zone and destroy targets but at much higher cost and increased duration of the conflict.

Conclusion

Attempts to penetrate an A2/AD zone of a near-peer competitor are possible, but at high cost and over a prolonged conflict. By utilizing space- and aero-stat-based ISR, a defender gains a nearly indestructible early warning system. It can protect his ground-based search radars while maintaining situational awareness. EW reconnaissance systems and high-power computers can distinguish decoys from real aircraft. This degrades the attacker's situational awareness because the defending battery no longer emits until it is ready to engage real targets. The real defenses are camouflaged, and realistic decoys are set up to draw fire away from defensive systems. The attacker is then engaged from unexpected locations by modern air defenses, including long-range surface-to-air missiles and fixed-wing fighter aircraft.

The defenders will fight in a decentralized manner. Also, a defender's higher headquarters will allocate ADA and antiship assets and allow them to fight on their own with direct access to early warning networks. The higher headquarters will likely retain control of defending air assets and allocate targets for their own long-range fires, but the bulk of the fight will be in a decentralized manner. This will make dis-integrating enemy defenses difficult because C2 centers will not affect the fight to the degree seen in previous conflicts. Destroying the

defender's C2 nodes will degrade but not dis-integrate the defense. Furthermore, the enemy will likely regenerate damaged C2 nodes, while networked communications will continue to function unabated due to multiple connections and non-C2 nodes that carry the same traffic.

Penetration and degradation of an A2/AD zone is possible through converging key systems across all domains. The real challenge lies in dis-integration of the A2/AD zone. It is important not to underestimate the resilience of enemy networks and their ability to reconstitute damage inflicted by U.S. fire power. At the strategic level, failure to gain quick victory via dis-integration of A2/AD zones will result in a war of attrition, a contest that may not be won at a politically acceptable cost, ending the conflict in a peace settlement favorable to the adversary. JFQ

Notes

¹ Eugene Gholz, "What Is A2/AD and Why Does It Matter to the United States?" discussion, Army Navy Club, Washington, DC, September 15, 2019.

² The Arab-Israeli War of 1973 was an exception. The Israeli air force was diverted to provide close air support to the army, repelling an Arab surprise ground attack, and did not have the time or resources to suppress Arab air defense artillery first.

³ Tim Fernholz, "The Company Photographing Every Spot of Land on Earth, Every Single Day," *Quartz*, November 11, 2017, available at <<https://qz.com/1126301/the-company-photographing-every-spot-of-land-on-earth-every-single-day/>>.

⁴ Will Marshall, "Mission 1 Complete," *Planet.com*, November 9, 2017, available at <www.planet.com/pulse/mission-1/>.

⁵ *Program Acquisition Cost by Weapon System: United States Department of Defense Fiscal Year 2018 Budget Request* (Washington, DC: Department of Defense, May 2017).

⁶ Patrick Tucker, "Russia Claims It Now Has Lasers to Shoot Satellites," *Defense One*, February 26, 2018, available at <www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/>.

⁷ "High Altitude Airship (HAA)," *Global Security*, available at <www.globalsecurity.org/intell/systems/haa.htm>.

⁸ Makena Kelly, "Google Hired Microworkers to Train Its Controversial Project Maven AI," *The Verge*, February 4, 2019, available at <www.theverge.com/2019/2/4/18211155/>

google-microworkers-maven-ai-train-pentagon-pay-salary>.

⁹ Samuel Bendett, "America Is Getting Outclassed by Russian Electronic Warfare," *The National Interest*, September 19, 2017, available at <<https://nationalinterest.org/feature/america-getting-outclassed-by-russian-electronic-warfare-22380>>; also see Vladimir Tuchkov, "U.S. General: 'We Are Powerless before Russian Krasukha and Moskva,'" *SVPRESSA*, August 28, 2017, available at <spresso.ru/war21/article/180142/>.

¹⁰ Yuen Yiu, "Is China the Leader in Quantum Communications?" *Inside Science*, January 19, 2018, available at <www.insidescience.org/news/china-leader-quantum-communications>.

¹¹ Valeri Gerasimov, "Vectors of the Development of Military Strategy," *Krasnaya Zvezda* (Moscow), March 4, 2019, available at <<http://redstar.ru/vektory-ravzvitiya-voennoj-strategii/?attempt=1>>.

¹² Ibid.

¹³ "ISI First to Analyze Shayrat Airfield Missile Attack," *ImageSat International*, April 7, 2017, available at <<https://web.archive.org/web/20170413234913/http://www.imagesatintl.com/us-strike-syria/>>.

¹⁴ Bendett, "America Is Getting Outclassed by Russian Electronic Warfare."

¹⁵ Josie Ensor, "Syrian Warplanes Take Off Once Again from Air Base Bombed by U.S. Tomahawks," *Daily Telegraph* (London), April 8, 2017, available at <www.telegraph.co.uk/news/2017/04/08/syrian-warplanes-take-air-base-bombed-us-tomahawks/>.

¹⁶ Jeremy Binnie, "Russia Displays Cruise Missiles 'Shot Down' in Syria," *Janes*, April 26, 2018.

¹⁷ "Russian Military Shows Wreckage of Missiles Intercepted in Syria, Says Two Unexploded Missiles Delivered to Moscow," *Southfront*, April 25, 2018, available at <<https://southfront.org/russian-military-shows-wreckage-of-missiles-intercepted-in-syria-says-two-unexploded-delivered-to-moscow/>>.

¹⁸ Jessica Finn and Jennifer Smith, "Royal Navy's \$1.3bn Submarine Was Locked in a Deadly Game of 'Hide and Seek' with Russian Hunter-Killer Ships for Days before Air Strikes on Syria," *Daily Mail* (London), April 15, 2018, available at <www.dailymail.co.uk/news/article-5617799/Royal-Navy-submarine-hunted-Russia-cat-mouse-pursuit.html>.

¹⁹ *Program Acquisition Cost by Weapon System*.

²⁰ "Tomahawk (missile)," available at <[https://en.wikipedia.org/wiki/Tomahawk_\(missile\)](https://en.wikipedia.org/wiki/Tomahawk_(missile))>.

²¹ Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (Washington, DC: Department of Defense, September 2018), available at <<http://defense.gov/StrengtheningDefenseIndustrialBase>>.

²² James Holland, *Fortress Malta: An Island Under Siege, 1940–43* (New York: Hyperion, 2003).

²³ Jared Keller, "The Navy Says Its F-35C Is Ready for a Fight. The Navy's Own Data Says Otherwise," *Task and Purpose*, March 20, 2019, available at <<https://taskandpurpose.com/navy-f35-mission-capable-rate>>.

²⁴ John Barry, "The Kosovo Cover-Up," *Newsweek*, May 14, 2000, available at <www.newsweek.com/kosovo-cover-160273>.

²⁵ Sébastien Roblin, "Stealth Can Be Defeated: In 1999, an F-117 Nighthawk Was Shot Down," *The National Interest*, November 2, 2018, available at <<https://nationalinterest.org/blog/buzz/stealth-can-be-defeated-1999-f-117-nighthawk-was-shot-down-35142>>.

²⁶ Alexsey Ramm and Evgeny Andreev, "The Ministry of Defense Returned the 'Inflatable' Regiment," *IZ.ru*, September 22, 2017, available at <<https://iz.ru/634072/aleksei-ramm-evgenii-andreev/minoborony-vernu-lo-naduvnoi-polku>>.

²⁷ "Russian Inflatable Weapons," BBC, video, 1:38, December 22, 2012, available at <www.youtube.com/watch?v=PpVqttw0ig8>.

²⁸ "Inflatable Tank in Syria Hit by American ATGM," video, 0:33, March 17, 2018, available at <www.youtube.com/watch?v=MIKEZMkJM8M>.

²⁹ Robert Beckhusen, "The Russian Army Is Inflating Giant Dummy Tanks," *The National Interest*, December 1, 2017, available at <<https://nationalinterest.org/blog/the-buzz/the-russian-army-inflating-giant-dummy-tanks-23445>>.

³⁰ See "Club-K: Container Missile System," Rosoboronexport, available at <<http://roe.ru/eng/catalog/naval-systems/shipborne-weapons/klab-k/>>; Bill Gertz, "China Building Long-Range Cruise Missile Launched from Ship Container," *Washington Free Beacon*, March 27, 2019, available at <<https://freebeacon.com/national-security/china-building-long-range-cruise-missile-launched-from-ship-container/>>.

³¹ Tyler Rogoway, "Northrop Grumman Shows Off Shipping Container-Launched Anti-Radiation Missile Concept," *The Drive*, October 8, 2018, available at <[www.thedrive.com/the-war-zone/24111/northrop-grumman-shows-off-shipping-container-launched-anti-radiation-missile-concept](http://thedrive.com/the-war-zone/24111/northrop-grumman-shows-off-shipping-container-launched-anti-radiation-missile-concept)>.



Soyuz-2.1b rocket lifts off from Baikonur Cosmodrome in Kazakhstan, together with 34 OneWeb communication satellites
(Courtesy Roscosmos)

Proliferated Commercial Satellite Constellations

Implications for National Security

By Matthew A. Hallex and Travis S. Cottom

The falling costs of space launch and the increasing capabilities of small satellites have enabled the emergence of radically new space architectures—proliferated constellations made up of dozens, hundreds, or even thousands of satellites in low orbits.

Commercial space actors—from tiny startups to companies backed by billions of dollars of private investment—are pursuing these new architectures to disrupt traditional business models for commercial Earth observation and satellite communications. The success

of these endeavors will result in new space-based services, including global broadband Internet coverage broadcast from orbit and high-revisit overhead imagery of much of the Earth's surface.

The effects of proliferated constellations will not be confined to the commercial sector. The exponential increase in the number of satellites on orbit will shape the future military operating environment in space. The increase in

Matthew A. Hallex is a Research Staff Member at the Institute for Defense Analyses. Travis S. Cottom is a Research Associate at the Institute for Defense Analyses.

the availability of satellite imagery and communications bandwidth on the open market will also affect the operating environment in the ground, maritime, and air domains, offering new capabilities that can address hard problems facing the U.S. military, such as tracking mobile targets, operating in the Arctic, or providing resilient space support in the face of growing counterspace threats. These trends will also create new challenges as adversaries ranging from Great Power competitors to hostile nonstate actors gain cheap access to space capabilities and the emergence of space-based Internet reshapes the cyber battlespace.

This article discusses some of the proposed commercial proliferated constellations being developed in the United States and abroad and explores the potential effects of proliferated constellations on the space, terrestrial, and cyber domains. It identifies the multidomain challenges and opportunities these trends create for the warfighter and proposes steps that the Department of Defense (DOD) and the broader national security community can take to prepare.

Emerging Commercial Proliferated Satellite Constellations

Commercial proliferated constellations will change how satellite communications and Earth observation services are provided. Not all the projects detailed below will enter service. The total market for high bandwidth communications is estimated to reach 3 terabits of data by 2024. If all the projected proliferated communications constellations and other projected satellite communications services become accessible, 20 to 30 terabits will be available by that year. The small satellite imagery market is expected to grow from its very small base, but government customers still dominate the demand for satellite imagery.¹ In addition to potential limits on demand, some industry experts have raised concerns about shortages in investment capital necessary to complete various competing efforts, and other critics have compared the current era to the failures of the large, disaggre-

Table 1. Planned Proliferated Communications Constellations

Satellite Operator	Proposed Satellites	Satellite Design Life (Years)
OneWeb	> 2,000	7–10
SpaceX Starlink	~ 12,000	5–7
Boeing	> 3,000	10–15
Telesat	292–512	10
Kepler Communications	140	10
LEOSat	84	10

Sources: Tereza Pultarova and Caleb Henry, "OneWeb Weighing 2,000 More Satellites," SpaceNews (February 24, 2017); Jon Brodkin, "FCC Tells SpaceX It Can Deploy Up to 11,943 Broadband Satellites," Ars Technica (November 15, 2018); Grant R. Cates, Daniel X. Houston, Douglas G. Conley, and Karen L. Jones, "Launch Uncertainty: Implications for Large Constellations," *The Aerospace Corporation*, November 2018, 2; Caleb Henry, "Telesat Says Ideal LEO Constellation Is 292 Satellites, but Could Be 512," SpaceNews (September 11, 2018).

gated Teledesic constellation and the struggles of Iridium in the 1990s.²

Growing global demand for information services, the greater availability of capital compared to previous eras of commercial satellite growth, the increasing affordability of access to space launch, and greater economies of scale in producing small satellites, however, may make proliferated constellations more viable commercial endeavors. The availability of space-based broadband communications, for instance, will likely drive the growth of Internet-of-Things applications leading to further demand for communications services. Even if only a handful of proliferated constellation efforts succeed, it will produce both a paradigm shift in how space services are provided and a substantial growth in the number of satellites on orbit.

Communications

Satellites in geosynchronous orbit (GEO) have traditionally provided satellite communications where satellites can broadcast to large areas of the Earth. These satellites have provided low data rates and relatively high latency communications, good enough for niche applications but not competitive with fiber optics and other terrestrial alternatives for broadband communications. Proliferated communications constellations, often referred to as mega-constellations because of their size, are in low-Earth orbit (LEO) and aim to provide high bandwidth, low latency communications

competitive with terrestrial broadband communications. This will not only allow satellite communications to compete for long-distance backhaul and mobile users but also address underserved populations. Much of the developing world lacks access to terrestrial broadband infrastructure, and 57 percent of the global population does not have access to the Internet.³ Mega-constellations could allow the developing world to skip laying costly fiber-optic cable in the same way the proliferation of cellular phone technology provided communications without the need to build phone lines in the developing world. LEO-proliferated constellations will also be able to provide communications to high-latitude populations in Alaska, northern Canada, Scandinavia, and Russia, which are poorly served by terrestrial communications infrastructure and outside the coverage of GEO communications satellites.⁴

OneWeb and SpaceX are pursuing the most ambitious proposals for LEO communications proliferated constellations (see table 1). OneWeb has raised more than \$1.7 billion in investments to build a first-generation constellation of 648 satellites, expected to enter commercial service by 2020, and plans to expand the constellation with 2,000 satellites in the future.⁵ Plans for SpaceX's Starlink proliferated constellation are even more ambitious. The first generation of Starlink is planned to consist of

Table 2. Planned Proliferated Earth Observation Constellations

Satellite Operator	Proposed Satellites	Resolution
Planet	~150	0.72m–5m
Spaceflight Industries	60	1m
Satellogic	300	1m
Hera Systems	48	.5m
UrtheCast	16	0.75m–22m
Capella Space	30	1-30m SAR
Canon	>100	1m
DigitalGlobe	6	0.3m

Sources: "Planet Imagery and Archive," *Planet.com*; Jeff Foust, "Spaceflight Raises \$150 Million for BlackSky Constellation," *Space News*, March 13, 2018; Caleb Henry, "Satellogic on Its Way to Launching 300 Satellite Constellation for Earth Observation," *Satellite Today*, March 17, 2016; Bhavya Lal et al., *Global Trends in Small Satellites* (Washington, DC: IDA Science and Technology Institute, July 2017); "Sensor Technologies," *UrtheCast.com*; Nobutada Sako, "Utilizing Commercial DSLR for High Resolution Earth Observation Satellite," paper presented at the AIAA/USU Conference on Small Satellites, Logan, UT, August 2018, 1–3; "CE-SAT 1," *Space Flight 101*; Stephen Clark, "DigitalGlobe Books Two Launches with SpaceX for Earth-Imaging Fleet," *Spaceflight Now*, March 28, 2018.

more than 4,000 satellites, and SpaceX has secured U.S. Government approval for a final constellation of almost 12,000 satellites.⁶ Other proliferated constellation proposals have come from established companies such as Boeing and Canada's Telesat, as well as smaller startups like Kepler Communications and LeoSat.⁷ While these are only nascent projects, the potential for large quantities of communications bandwidth entering the market from LEO communications mega-constellations, as well as smaller numbers of high-throughput GEO communications satellites, have led traditional satellite communications providers to delay purchasing new and replacement communications satellites that could struggle to compete in the future business environment.

Earth Observation

The Earth observation market has already moved toward commercial constellations of large numbers of small satellites. While these constellations are smaller than planned communications mega-constellations, ranging from dozens to hundreds of satellites, this disaggregation of commercial space capability has increased access to Earth observation capabilities useful for national security applications.

The most mature of the disaggregated Earth observation constellations are those operated by Planet and Spire Global. By the end of 2017, Planet operated a constellation of 140 Dove imagery CubeSats, 5 RapidEye medium-resolution, and 13 higher resolution SkySat satellites that can image Earth's entire landmass daily.⁸ In July 2018, Spire operated 61 of its Lemur satellites (out of a planned 125) that track the Automatic Identification System (AIS) beacons of ships that collect weather data by monitoring the radio occupation of GPS signals.⁹

Traditional remote-sensing providers such as Digital Globe and other larger, established companies including Canon, the Japanese manufacturer of cameras and other imagery products, are planning disaggregated imagery constellations (see table 2). Additional startup companies are also aiming to join the ranks of the more mature Earth observation constellations offering optical imagery, high-revisit, all weather, and nighttime Synthetic Aperture Radar,¹⁰ as well as radio signal collection satellites that can geolocate signals emissions—essentially offering commercial electronic intelligence capabilities that can support transportation and logistics, emergency search and rescue, or spectrum mapping in addition to its existing applications for

national security and other government purposes.¹¹

The U.S. Government has been the largest and most stable customer for commercial satellite imagery, including resources from new imagery proliferated constellations. For instance, a significant share of Planet's growth has been through multiple contracts with the National Geospatial-Intelligence Agency.¹² Commercial Earth observation companies, however, are seeking to diversify their customer base and reach new markets—to rely less on U.S. Government spending and, consequently, to potentially reduce its sway over commercial actors. With lower prices and increasingly on-demand imagery services, proliferated constellation companies are trying to focus on new, nontraditional satellite imagery markets: industrial monitoring, agriculture, utilities, marine transportation analytics, insurance, resource management, business intelligence, and other data-driven, decisionmaking practices.¹³ This broader range of services will help drive market expansion, and the Institute for Defense Analyses' Science and Technology Policy Institute projects the overall commercial small satellite imaging market will grow from \$15 million in 2015 to \$164 million in 2020.¹⁴

Foreign Proliferated Constellation Efforts

Interest in proliferated constellations is not confined to the United States and Western commercial space actors—both China and Russia are pursuing their own proliferated constellation projects. The development of foreign proliferated constellations will allow not only their owners to access these capabilities, but potentially access also to a wider range of actors. Given China's willingness to allow for commercial dealings with countries hostile to the United States, these systems could pose a significant threat to U.S. interests.

The state-owned China Aerospace Science and Technology Corporation (CASC) is planning the 300-satellite Hongyan LEO broadband communications proliferated constellation, and the



Airman with 707th Communications Squadron Special Missions Flight repairs connection on CubeSat, in Laurel, Maryland, January 2018 (U.S. Air Force/Alexandre Montes)

state-owned China Aerospace Science and Industry Corporation plans its own 156-satellite Xingyun communications constellation. The first Hongyan satellite was launched in late 2018, and CASC has established a factory in Tianjin capable of producing 130 satellites a year. In 2015, China launched the first of its Jilin commercial imagery satellites to complement the Gaofen civil imagery constellation. The Jilin constellation is planned to reach 60 satellites by 2020 in order to provide global, 30-minute revisit rates, and then 138 satellites by 2030 to obtain 10-minute revisit rates worldwide.¹⁵

While ostensibly commercial, because China has raised private funds and intends to sell products and services to stakeholders beyond the government, Chinese proliferated constellations are likely to be less responsive to market pressures than Western commercial proliferated constellations. China is pursuing

commercial space capability to bolster its military and civil space systems as part of its policy of “civil-military fusion,” making militarily useful proliferated constellations likely candidates for government support.¹⁶ Chinese proliferated constellations are also likely to be able to rely on government financing and other support to offer services to emerging markets in Africa, Central Asia, and Latin America as part of China’s One Belt, One Road development and trade initiative.¹⁷

Russia also has proliferated constellation aspirations. Roscosmos, the Russian state-owned space corporation, has announced plans to build the 288-satellite Efir constellation to provide global broadband Internet by 2025. This project is part of a larger projected proliferated constellation comprising 600 communications and optical imagery satellites to provide global coverage from low orbits.¹⁸ Given the difficulties facing

the Russian civil and commercial space programs in recent years, Russia is a less likely proliferated constellation competitor than China.

Spillover Effects: Satellite Manufacturing and Space Launch

The emergence of proliferated constellations is reshaping other areas of the commercial space world by driving expansion of satellite manufacturing and space launch capacity. The large numbers of satellites that comprise proliferated constellations require satellites to be mass-produced quickly and less expensively—a shift from the usual paradigm of uniquely designed, exquisite, and expensive space systems. To produce the hundreds of satellites that will make up the OneWeb constellation, Airbus has opened a production line in Toulouse, France, and is planning an

additional high-capacity satellite manufacturing plant in Florida.¹⁹ In August 2018, Boeing agreed to acquire Millennium Space Systems, which is building a manufacturing center in California that will annually produce hundreds of small satellites.²⁰ Similarly, in 2018, Planet opened a facility in San Francisco that can produce 40 small imagery satellites each week.²¹

The deployment of proliferated constellations will continue to drive demand for space launch capacity. Small satellites have traditionally been launched as rideshare or secondary payloads, but the demand for these opportunities exceeds the rate of large payload launches. Rideshare opportunities also bound a satellite to the orbit of the primary satellite, which may not be the optimal inclination or orbit for smaller satellites. The lack of rideshare availability is driving the small launch vehicle market; companies such as Vector Launch, Rocket Lab, Firefly Aerospace, and Virgin Orbit are developing new vehicles to capture part of this demand. China also has an active small launch program with three operational small launch vehicles.²²

Demand is not confined to small launch vehicles. Larger launch vehicles will permit proliferated constellations to be rapidly deployed by manifesting dozens to hundreds of small satellites in a single launch. For instance, in February 2017, Planet launched 88 Dove satellites on a single Indian Polar Satellite Launch Vehicle.²³ The relatively short planned lifespan of proliferated constellation satellites will also result in a continuous demand for launch services to replace satellites as they end their service lives, potentially resulting in larger economies of scale that reduce the cost of all launches.

Proliferated Constellations and National Security

While commercial interest is driving the development of proliferated constellations, these new space architectures can provide capabilities previously available only to a few spacefaring great powers. These new useful capabilities will not only be available to the United States.

China wants to build its own proliferated constellations for communications and surveillance. The development of proliferated constellations will further the democratization of space; capabilities will become cheaper and more readily available to a range of state and nonstate actors.²⁴ Adapting to the emergence of proliferated constellation is not simply a problem for space warfighters. It requires a joint multidomain solution to take advantage of the operational opportunities provided by these systems and to address the new threats in the space, air, maritime, land, and cyber domains detailed below.

Satellite Proliferation and Space Security

The space operational environment is increasingly congested, contested, and competitive. The emergence of satellite proliferated constellations will accelerate these trends but will also offer opportunities for the United States to better deter adversaries from initiating conflicts and to address growing adversary counterspace capabilities.

The OneWeb satellite constellation alone would increase the number of operational satellites by almost 50 percent compared to today, and the SpaceX constellation would triple the number of operational satellites compared to today.²⁵ The addition of hundreds or thousands of proliferated constellation satellites would increase congestion, stress existing U.S. space situational awareness (SSA) and space traffic management capabilities, and could create a more dangerous debris environment. More satellites and associated debris would threaten orbital safety and, at the very least, increase the number of conjunction warnings—notices of possible collisions between satellites and other objects in space—that the Combined Space Operations Center issues, distracting it from its national security mission.

Proliferated constellation operators intend to address the risk of debris from their satellites by ensuring that they are disposed of through atmospheric re-entry at the end of their operating lives. A recent study by the National Aeronautics and Space Administration's Orbital

Debris Program Office suggests that a 99 percent end-of-life disposal rate may be necessary to maintain a sustainable orbital environment.²⁶ The disposal level for LEO satellites, however, has not reached 20 percent in any of the last 25 years.²⁷ Unless proliferated constellations become far more reliable, they could pose a long-term threat to the ability of the United States and other space actors to operate safely in space.

While potentially threatening the sustainability of safe orbital operations, new proliferated constellations also offer opportunities for the United States to increase the resilience of its national security space architectures. Increasing the resilience of U.S. national security space architectures has strategic implications beyond the space domain. Adversaries such as China and Russia see U.S. dependence on space as a key vulnerability to exploit during a conflict. Resilient, proliferated satellite constellations support deterrence by denying adversaries the space superiority they believe is necessary to initiate and win a war against the United States.²⁸ Should deterrence fail, these constellations could provide assured space support to U.S. forces in the face of adversary counterspace threats while imposing costs on competitors by rendering their investments in counterspace systems irrelevant. Proliferated constellations can support these goals in four main ways.

First, the extreme degree of disaggregation inherent in government and commercial proliferated constellations could make them more resilient to attacks by many adversary counterspace systems. A constellation composed of hundreds or thousands of satellites could withstand losing a relatively large number of them before losing significant capability. Conducting such an attack with kinetic antisatellite weapons—like those China and Russia are developing—would require hundreds of costly weapons to destroy satellites that would be relatively inexpensive to replace.

Second, proliferated constellations would be more resilient to adversary electronic warfare. Satellites in LEO can emit signals 1,280 times more powerful than signals from satellites in GEO.²⁹ They



SpaceX Falcon 9 rocket launches Starlink at Cape Canaveral Air Force Station, Florida, on May 23, 2019, putting 60 satellites into orbit (U.S. Air Force/Alex Preisser)

also are faster in the sky than satellites in more distant orbits, which, combined with the planned use of small spot beams for communications proliferated constellations, would shrink the geographic area in which an adversary ground-based jammer could effectively operate, making jammers less effective and easier to geolocate and eliminate.³⁰

Third, even if the United States chooses not to deploy national security proliferated constellations during peacetime, industrial capacity for mass-producing proliferated constellation satellites could be repurposed during a conflict. Just as Ford production lines shifted from automobiles to tanks and aircraft during World War II, one can easily imagine commercial satellite factories building military reconnaissance or communications satellites during a conflict.

Fourth, deploying and maintaining constellations of hundreds or thousands

of satellites will drive the development of low-cost launches to a much higher rate than is available today. Inexpensive, high-cadence space launch could provide a commercial solution to operationally responsive launch needs of the U.S. Government. In a future where space launches occur weekly or less, the launch capacity needed to augment national security space systems during a crisis or to replace systems lost during a conflict in space would be readily available.³¹

The Fight on Earth: Opportunities and Threats

The emergence of proliferated constellations will lead to easier access to satellite communications, space imagery, and other capabilities that can support U.S. and adversary military operations in the ground, maritime, and air domains. Adapting to these changes will likely require the development of

new joint operational concepts to better exploit space systems in support of the joint fight as well as address new force protection challenges when fighting space-enabled state and nonstate actors.

Proliferated constellations will substantially increase the availability of communications bandwidth for military operations. These satellites would provide high bandwidth to forces with less latency than existing GEO satellites,³² which, in turn, would improve access to reachback communications to forward-deployed military forces, and would also help meet the growing demand for transfer capacity for data collected by unmanned systems and other forward sensors.

Proliferated LEO communications constellations would also offer coverage in theaters that are poorly served by commercial satellite communications today. Satellites in GEO do not sufficiently support operations in the Arctic



Marines lower RQ-21A Blackjack unmanned aerial system from recovery system aboard USS *John P. Murtha*, Gulf of Aden, July 2019 (U.S. Marine Corps/Adam Dublinske)

and other high-latitude regions that are growing in economic and national security importance.³³ Similarly, naval and air forces operating in the Pacific theater have less access to commercial communications than other theaters due to the lack of commercial customers in the open ocean. Proliferated commercial LEO constellations would provide greater communications handling in both regions because of their global coverage.

While unable to provide the high-resolution imagery and other specialized capabilities of existing national security satellites, proliferated LEO constellations could help to address some of the intelligence challenges the U.S. military faces. During the first Gulf War, the United States was unable to track and target Iraq's Scud missile systems despite enjoying almost total air superiority. Since then, mobile missiles and other elusive targets have multiplied as potential adversaries seek to defeat U.S. conventional precision and nuclear strike systems. Imagery proliferated constellations could provide continuous or near-continuous coverage of missile operating areas to better enable the United States to find and eliminate these threat systems.

The near continuous imagery coverage proliferated constellations offers—particularly if they include radar

satellites that can see through clouds—combined with ground processing capabilities that can automatically detect changes in imagery would also make adversary deception operations less effective.³⁴ Because the United States is likely to be on the defensive in the most worrying scenarios for conflict—such as defending allies in Eastern Europe or East Asia—these new capabilities will support U.S. efforts to detect adversary mobilization and to avoid operational surprise.

Of course, these new capabilities will also be available to potential adversaries. The development of proliferated constellations allows other nations to replicate the U.S. ability to support space global power projection. The global coverage LEO communications constellations enable would also allow China to support forces deployed far from its mainland, including ships deep in the Pacific or deployed to Djibouti or elsewhere in Africa.

These capabilities will also heighten the challenge of protecting U.S. forces and bases. High-revisit commercial imagery could also track mobile targets like U.S. naval vessels or U.S. aircraft using smaller “adaptive bases” in Europe or the Pacific to avoid attack. In support of its “counter-intervention” strategy, China, like the Soviet Union before it, has invested substantially in optical imagery,

radar, and electronic intelligence satellites in order to track U.S. carrier groups. Chinese commercial imagery proliferated constellations would bolster these capabilities and provide a resilient capability to track U.S. forces worldwide.

Nonstate actors will also be able to conduct global surveillance using commercial proliferated constellations. Global Fishing Watch, an environmental nonprofit organization that aims to reduce overfishing, already uses commercial satellites as part of what is essentially a space-based kill chain to eliminate environmental crime at sea.³⁵ It monitors AIS beacons that seagoing vessels are required to carry to track their locations to avoid collisions. When they detect unusual behavior, such as ships turning off their AIS signals, they use Planet’s imagery constellation to locate the ship and then cue higher resolution satellites to collect images of illegal activity. Hostile actors with goals less noble than environmental conservation—such as pirates, antiship missiles, or armed Houthi rebels—could use commercial proliferated constellations to track and target ships at sea with similar effectiveness.

Space Internet and the Cyber Battlespace

Proliferated constellations may also shape the future cyber battlespace by supplanting the traditional physical infrastructure that underlies the Internet and creating a new orbital layer for cyber operations.

Today, more than 90 percent of Internet traffic is carried by undersea fiber optic cables that stretch over thousands of miles of ocean floor. These cables are vulnerable to accidental cuts and are likely targets of enemy action during wartime. Speaking at the opening of SpaceX's Seattle location in 2015, Elon Musk highlighted SpaceX's goal of carrying “more than half of the long-distance traffic” on its satellite network.³⁶ Satellite constellations would become increasingly critical infrastructure for the U.S. and global economy if they facilitated a larger share of global telecommunication traffic.

Ownership of the infrastructure that underlies the Internet can produce

intelligence and cyber warfighting advantages. Analysts have raised concerns over the cyber security implications of the increasing number of Chinese companies that own and operate long-distance fiber optic cables. Chinese commercial proliferated constellations could augment these cables to compete for global Internet traffic, exacerbating the trend identified by Eric Schmidt, former Google CEO, of a bifurcation into Chinese and non-Chinese Internets that operate on different infrastructure, standards, and levels of government control.³⁷

Proliferated constellations themselves are a likely target for cyber operations. The mass production of satellites for a proliferated constellation could easily result in the cyber vulnerabilities of any particular satellite replicating across a network, making it easier to attack the entire architecture. It may also be easier to carry out a cyber attack on satellites intended to directly interface with the Internet than on satellites that require more specialized communications interfaces.³⁸ The challenge of attacking proliferated constellations with kinetic counterspace weapons may lead adversaries to a greater reliance on cyber threats against U.S. national security and commercial space architectures. As the joint force makes greater use of proliferated satellite constellations, cyber defense of U.S. and commercial satellite systems will likely become an increasingly important mission.

A Path Forward for DOD

Making use of the new capabilities provided by proliferated satellite constellations and addressing the threats posed by new adversary space capabilities is not a niche issue for space warfighters. Adapting to the future that these new space capabilities will create requires a joint, multidomain effort. The heart of this effort should be a joint campaign of experimentation—including wargaming, discovery exercises, and prototyping—that develops understanding of the challenges and opportunities proliferated constellations create for warfighters in space and other domains, to develop new operational concepts to make U.S. forces more capable and lethal in this

future, and to better understand the strategic consequences that shifting balances in space and other domains will have for the competitive balance among the United States, China, Russia, and other space-enabled state and nonstate threats.³⁹

Potential starting points for this effort include examining how best to integrate new communications and intelligence, surveillance, and reconnaissance (ISR) capabilities at the tactical level, and what kind of denial and deception capabilities will best enable U.S. operations in a future characterized by ubiquitous orbital surveillance. Experimentation need not be limited to tabletop exercises or simulations—the lower cost of manufacturing and launching space systems will allow DOD to operate more on-orbit experiments. Along with demonstrating and maturing new space technologies, DOD can make greater use of prototype space systems and architectures to support field exercises and experiments aimed at discovering how best to use these new space technologies to support U.S. forces.

A joint, multidomain campaign of experimentation will also help to define new requirements for DOD use of proliferated satellite constellations. This should help DOD determine the best path to making use of new space capabilities and the balance between acquiring DOD-operated satellites and improving engagement with industry to make better use of the commercial proliferated satellite capabilities discussed above.

This could involve DOD deploying its own proliferated constellations. The Space Development Agency (SDA), established in 2019, aims to develop proliferated constellations that can provide communications, ISR, missile warning, and an alternative to legacy GPS satellites.⁴⁰ The SDA builds on existing efforts to leverage emerging commercial constellations such as the Defense Advanced Research Projects Agency's Blackjack program.⁴¹ These efforts would produce new satellites to augment existing national security architecture, but at a much lower cost, and could allow for fast and inexpensive expansion of U.S.

military space capabilities in response to new threats.

In addition to developing and deploying its own satellites, DOD could improve its engagement with the industry to better capitalize on capabilities offered by new commercial proliferated architectures. The Defense Department has strong ties with traditional aerospace companies, some of which are part of the manufacture and launch of proliferated constellations. Many of these new space systems, however, are being developed by small and agile startup companies—Silicon Valley tech companies that build satellites rather than apps—that DOD has struggled to connect with. A key part of the effort to improve DOD's relationship with Silicon Valley and its broader ability to harness commercial innovation is improving the acquisitions process. Commercial proliferated constellation operators aim to offer data and information services rather than the raw imagery or transponder leases of traditional commercial space operators. These companies also aim to move quickly—inexpensive, rapidly manufactured, frequently launched satellites with short lifespans that enable rapid technology refresh and evolution of capability. DOD processes need to move at the speed of the commercial sector to exploit these new space services or to develop U.S. Government proliferated constellations to meet military and intelligence needs. One step in this direction would be the expanded use of waivers that allow venture capital funded companies to participate in DOD Small Business Innovation Research contracts they are otherwise excluded from.⁴²

In addition to developing space capabilities to address the needs of the joint warfighter, DOD needs to prepare for new requirements for SSA and space traffic management resulting from increases in satellites and debris on orbit. Beyond investing in new military capabilities, the Defense Department should consider investments to improve the integration of foreign and commercial SSA data into its systems. Alternatively, DOD could support the transfer of space traffic management responsibilities to a civilian

agency, which would reduce the burden on existing military organizations.⁴³

The Defense Department can also play a large role in shaping the future commercial space environment by protecting commercial proliferated constellations and related technologies from interference by foreign companies and governments. It should be prepared to address the failures of commercial proliferated constellation efforts and to act to maintain the viability of commercial constellations with particular strategic value.

Acquiring access to technologies developed by U.S. companies is a key part of China's long-term strategy to match U.S. economic and military power. Tactics include hacking, industrial espionage, and investments in U.S. technology startups. DOD should push to improve the whole-of-government approach to protecting U.S. technologies and expanded use of existing tools for monitoring and blocking foreign efforts to acquire strategic technologies from the United States. For instance, foreign investments in the operators and manufacturers of commercial proliferated constellations should be an ongoing priority for review by the Committee on Foreign Investment in the United States, the interagency committee with the power to regulate foreign investment that could threaten U.S. national security. DOD could also include commercial constellation operators in the new Trusted Capital Marketplace, which links companies crucial to defense supply chains with trusted sources of commercial investment.⁴⁴

The DOD part in preserving Iridium—the \$5 billion LEO communications constellation that was a forerunner of today's emerging proliferated constellations—exemplifies another role it could play in managing the future commercial environment. When Iridium faced bankruptcy in 1999, its corporate parent Motorola planned to deorbit the satellites to avoid risking future liability resulting from satellite collisions. The DOD offer to indemnify Motorola against future liability, as well as a multimillion-dollar, 2-year contract for communications services, allowed

Iridium to restructure its debt through bankruptcy. This intervention enabled Motorola to spin off Iridium as an independent company that has since become economically viable and provides vital communication services to U.S. forces around the world.⁴⁵ As commercial proliferated constellations enter service, DOD should identify systems with particular military value and use its unique role as one of the largest consumers of space services to preserve capabilities in case a future economic downturn threatens the viability of strategic commercial capabilities. JFQ

Notes

¹ Bhavya Lal et al., *Global Trends in Small Satellites* (Washington, DC: IDA Science and Technology Policy Institute, July 2017), 3-4, 3-7.

² Debra Werner, "Analysts See Demand for Two or Three Megaconstellations," *Space News*, October 9, 2018, available at <<https://spacenews.com/megaconstellation-demand/>>; Caleb Henry, "LEO and MEO Broadband Constellations Mega Source of Consternation," *Space News*, March 13, 2018, available at <<https://spacenews.com/divining-what-the-stars-hold-in-store-for-broadband-megaconstellations/>>.

³ Sarah Scoles, "SpaceX Wants to Launch Thousands of Satellites. What on Earth For?" *Wired*, June 8, 2017, available at <www.wired.com/story/spacex-wants-to-launch-thousands-of-satellites-what-for/>. Mega-constellations in low-Earth orbit plan to offer latency on the order of 30 milliseconds (ms), comparable to the 10–50 ms latency of terrestrial fiber systems, and far lower than the ~600 ms latency of geosynchronous orbit communications satellites. See Ward A. Hanson, "Satellite Internet in the Mobile Age," *New Space* 4, no. 3 (September 2016), 143; Jon Brodkin, "Low-Latency Satellite Broadband Gets Approval to Serve U.S. Residents," *Ars Technica*, June 23, 2017, available at <<https://arstechnica.com/information-technology/2017/06/low-latency-satellite-broadband-gets-approval-to-serve-us-residents/>>.

⁴ Hanson, "Satellite Internet in the Mobile Age," 148.

⁵ Tereza Pultarova and Caleb Henry, "OneWeb Weighing 2,000 More Satellites," *Space News*, February 24, 2017, available at <<https://spacenews.com/oneweb-weighing-2000-more-satellites/>>; Mark Holmes, "Greg Wyler, the Definitive 2018 Interview," *Satellite Today* (December 2018), available at <<http://interactive.satellitetoday.com/>>

via/december-2018/greg-wyler-the-definitive-2018-interview/>.

⁶ Jon Brodkin, "FCC Tells SpaceX It Can Deploy Up to 11,943 Broadband Satellites," *Ars Technica*, November 15, 2018, available at <<https://arstechnica.com/information-technology/2018/11/spacex-gets-fcc-approval-for-7500-more-broadband-satellites/>>.

⁷ Chuck Black, "SpaceX, Telesat & Kepler Just Three of the Dozen Satellite Constellations Currently on the FCC Table," *Commercial Space*, November 20, 2016, available at <<http://acuriousguy.blogspot.com/2016/11/spacex-telesat-kepler-just-three-of.html>>.

⁸ Jeff Foust, "With 'Mission 1' Complete, Planet Turns Focus to Data Analysis," *Space News*, November 17, 2017, available at <<https://spacenews.com/with-mission-1-complete-planet-turns-focus-to-data-analysis/>>.

⁹ Caleb Henry, "From Silicon Valley to Singapore: Spire's Ambitious Remote Sensing Strategy," *Satellite Today*, September 25, 2014, available at <www.satellitetoday.com/innovation/2014/09/25/from-silicon-valley-to-singapore-spire-s-ambitious-remote-sensing-strategy/>.

¹⁰ See UrtheCast Web site, available at <www.urthecast.com/optisar/>; Jeff Foust, "Capella Space Raises \$19 Million for Radar Constellation," *Space News*, September 26, 2018, available at <<https://spacenews.com/capella-space-raises-19-million-for-radar-constellation/>>.

¹¹ See Hawkeye³⁶⁰ Web site, available at <www.he360.com/>.

¹² Caleb Henry, "Planet Wins Second NGA Satellite-Imagery Contract," *Space News*, July 20, 2017, available at <<https://spacenews.com/planet-wins-second-nga-satellite-imagery-contract/>>.

¹³ Narayan Prasad Nagendra and Tom Segret, "Challenges for NewSpace Commercial Earth Observation Small Satellites," *New Space* 5, no. 4 (December 2017), 242; Lal et al., *Global Trends in Small Satellites*, 3-6, 3-7.

¹⁴ Bhavya Lal et al., *Trends in Small Satellite Technology and the Role of the NASA Small Spacecraft Technology Program* (Washington, DC: IDA Science and Technology Policy Institute, March 28, 2017), 9.

¹⁵ "China to Set 300-Plus-Satellite Constellation to Serve Communication," Xinhua, February 23, 2018, available at <www.xinhuanet.com/english/2018-02/23/c_136994815.htm>; Andrew Jones, "Early Launch Plans for China's Hongyan LEO Communications Satellite Constellation Revealed," *GB Times*, March 12, 2018, available at <<https://gbtimes.com/early-launch-plans-for-chinas-hongyan-leo-communications-satellite-constellation-revealed/>>; Andrew Jones, "China to Launch First Satellite for Hongyan Global Internet Satellite Constellation on Saturday," *GB Times*, December 27, 2018, available at <<https://gbtimes.com/china-to-launch-first-satellite-for-hongyan-global-internet-satellite-con>>.

stellation-on-saturday>; Peter B. de Selding, “China Launches High-Resolution Commercial Imaging Satellite,” *Space News*, October 7, 2015, available at <<https://spacenews.com/china-launches-high-resolution-commercial-imaging-satellite/>>.

¹⁶ Lorand Laskai, “Civil-Military Fusion and the PLA’s Pursuit of Dominance in Emerging Technologies,” *China Brief* 18, no. 6 (2018), 12–16.

¹⁷ Jose Del Rosario, “China’s LEO Constellation Ambitions,” *Northern Sky Research*, March 7, 2018, available at <www.nsr.com/chinas-leo-constellation-ambitions/>.

¹⁸ “Russia to Create Orbital Internet Satellite Cluster by 2025,” TASS, May 22, 2018, available at <<http://tass.com/science/1005554>>; “Roscosmos: ‘Sphere’ Will Receive Elements of Artificial Intelligence,” TASS, June 12, 2018, available at <<https://tass.ru/interviews/5285285>>; Andrew Jones, “Jilin-1: China’s First Commercial Remote Sensing Satellites Aim to Fill the Void,” *GB Times*, May 12, 2016, available at <<https://gbtimes.com/jilin-1-chinas-first-commercial-remote-sensing-satellites-aim-fill-void>>.

¹⁹ Caleb Henry, “OneWeb Satellites to Keep Toulouse Factory Open for Other Customers,” *Space News*, September 12, 2017, available at <<https://spacenews.com/onestar-satellites-to-keep-toulouse-factory-open-for-other-customers/>>.

²⁰ Calvin Biesecker, “Boeing, Seeking an Entree into Small Satellite Market, to Acquire Millennium Space Systems,” *Defense Daily*, August 16, 2018, available at <www.defensedaily.com/boeing-seeking-entree-small-satellite-market-acquire-millennium-space-systems/>.

²¹ Will Marshall, “Planet Opens New State-of-the-Art Satellite Manufacturing Factory in San Francisco,” *Planet.com*, September 12, 2018, available at <www.planet.com/pulse/planet-opens-satellite-manufacturing-factory/>.

²² Carlos Niederstrasser, *Small Launch Vehicles—A 2018 State of the Industry Survey* (North Logan: Utah State University Research Foundation, 2018), 2.

²³ Robbie Schingler, “Planet Launches Satellite Constellation to Image the Whole Planet Daily,” *Planet.com*, February 14, 2017, available at <www.planet.com/pulse/planet-launches-satellite-constellation-to-image-the-whole-planet-daily/>.

²⁴ Dave Baiocchi and William Welser IV, “The Democratization of Space: New Actors Need New Rules,” *Foreign Affairs* (May/June 2015), available at <www.foreignaffairs.com/articles/space/2015-04-20/democratization-space>.

²⁵ Veronica L. Foreman, Afreen Siddiqi, and Olivier de Weck, “Large Satellite Constellation Orbital Debris Impacts: Case Studies of One-Web and SpaceX Proposals,” conference paper delivered at the American Institute of Aeronautics and Astronautics Space and Astronautics Forum and Exposition, Orlando, FL, September 12–14, 2017, 6.

²⁶ J.-C. Liou et al., “NASA ODPO’s Large Constellation Study,” *Orbital Debris Quarterly News* 22, no. 3 (September 2018), 4–5.

²⁷ Heiner Klinkrad, “Large Satellite Constellations and Related Challenges for Space Debris Mitigation,” *Journal of Space Safety Engineering* 4, no. 2 (July 2017), 6.

²⁸ For a discussion of Chinese and Russian counterspace intentions and capabilities, see *Challenges to Security in Space* (Washington, DC: Defense Intelligence Agency, January 2019).

²⁹ Paul Thomas, “Blackjack: Military Space Pivot to LEO,” presentation to the Future In-Space Operations Telecon, August 22, 2018, slide 7.

³⁰ Tyler G.R. Reid et al., “Leveraging Commercial Broadband LEO Constellations for Navigation,” in *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation* (Manassas, VA: Institute of Navigation, 2016), 2311.

³¹ Malcom Davis, “Elon Musk’s ‘BFR’ and 21st-Century Space War,” *The Strategist*, October 5, 2017, available at <www.aspistrategist.org.au/elon-musks-bfr-and-21st-century-space-war/>.

³² Anne Wainscott-Sargent, “LEO/MEO Satellites Poised to Make a Mark in Military Sector,” *Satellite Today*, February 12, 2018, available at <interactive.satellitetoday.com/leo-meo-satellites-poised-to-make-a-mark-in-military-sector/>.

³³ Andrew H. Boyd, *Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army*, Land Warfare Paper no. 115 (Arlington, VA: The Institute of Land Warfare, November 2017), 4–6.

³⁴ Adam G. Lenfestey et al., “Achieving Secrecy and Surprise in a Ubiquitous ISR Environment,” *Joint Force Quarterly* 88 (1st Quarter 2018), 85–90.

³⁵ Jeff Tarr and Will Marshall, “How Satellite Surveillance Is Hauling in Illegal Fishers,” World Economic Forum, October 3, 2017, available at <www.weforum.org/agenda/2017/10/satellites-illegal-fishing-digital-globe-planet/>.

³⁶ Elon Musk, “SpaceX Seattle 2015,” video, 25:53, January 2015, available at <www.youtube.com/watch?v=AHeZHyOnsm4>.

³⁷ Stacia Lee, “The Cybersecurity Implications of Chinese Undersea Cable Investment,” East Asia Center, Henry M. Jackson School of International Affairs, University of Washington, February 6, 2017, available at <jsis.washington.edu/eacenter/2017/02/06/cybersecurity-implications-chinese-undersea-cable-investment/>; Lora Kolodny, “Former Google CEO Predicts the Internet Will Split in Two—and One Part Will Be Led by China,” CNBC, September 20, 2018, available at <www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html>.

³⁸ Jason Fritz, “Satellite Hacking: A Guide for the Perplexed,” *Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (December 2012–May 2013), 26, 29–30.

³⁹ Kevin M. Woods and Thomas C. Greenwood, “Multidomain Battle: Time for a Campaign of Joint Experimentation,” *Joint Force Quarterly* 88 (1st Quarter 2018), 14–20; Tom Greenwood and Jim Greer, “Experimentation: The Road to Discovery,” *The Strategy Bridge*, March 1, 2018, available at <thestrategybridge.org/the-bridge/2018/3/1/experimentation-the-road-to-discovery>.

⁴⁰ David Vergun, “Space Development Agency Addresses Growing Capability Gaps,” Department of Defense, July 23, 2019, available at <www.defense.gov/explore/story/Article/1914120/space-development-agency-addresses-growing-capability-gaps/>.

⁴¹ Thomas, “Blackjack,” slides 6–7.

⁴² Sandra Erwin, “Thornberry Bill Would Help Venture-Backed Startups Compete for DOD Small Business Awards,” *Space News*, May 18, 2019, available at <spacenews.com/thornberry-bill-would-help-venture-backed-startups-compete-for-dod-small-business-awards/>.

⁴³ Owen Brown et al., *Orbital Traffic Management Study: Final Report* (Arlington, VA: SAIC, November 21, 2016), 25–28.

⁴⁴ “Department of Defense Press Briefing by Under Secretary of Defense Lord on DOD Acquisition Reforms and Major Programs,” Department of Defense, May 10, 2019, available at <dod.defense.gov/News/Transcripts/Transcript-View/Article/1844630/department-of-defense-press-briefing-by-under-secretary-of-defense-lord-on-dod/>.

⁴⁵ John Bloom, *Eccentric Orbits: The Iridium Story* (New York: Grove Press, June 2016), 346–357. While the capital costs of the initial Iridium constellation were erased through bankruptcy, Iridium has since been able to not only meet its operating expenses but also afford to recapitalize its space architecture by building and deploying the Iridium NEXT satellite constellation in early 2019.



Soldiers from Michigan National Guard form part of "enemy" force during simulated attack near Suwalski Gap as part of NATO exercise Saber Strike 2017, June 2017 (NATO)

Electronic Warfare in the Suwalski Gap

Facing the Russian "Accompli Attack"

By Jan E. Kallberg, Stephen S. Hamilton, and Matthew G. Sherburne

Dr. Jan E. Kallberg is an Assistant Professor of Political Science in the Department of Social Sciences at the United States Military Academy at West Point and a Research Scientist in the Army Cyber Institute (ACI) at West Point. Colonel Stephen S. Hamilton, USA, Ph.D., is an Academy Professor at West Point and the Technical Director of ACI. Major Matthew G. Sherburne, USA, is Mission Team Lead, 156 Cyber Protection Team, at 1st Cyber Battalion, Cyber Protection Brigade, Fort Gordon, Georgia.

The Joint Operating Environment 2035 predicts that for the foreseeable future, U.S. national interests will face challenges from both persistent disorders and states contesting international norms.¹ One of these outfalls could be "accompli" attacks from near-peer and peer states to exploit disorder, challenge international norms, and enjoy a quick advance with a limited resistance that cannot be realistically reversed. The rapid attack could establish territorial gains requiring a large-scale land war to liberate—with the imminent threat of an escalation to nuclear war—and the potentially massive cost in life, pain, and devastation to reverse the attacker's gains could be used to get negotiation leverage for the attacker in a final peace settlement. The attacker could also escalate the conflict once its territorial objectives are reached by declaring that a counteroffensive by the North Atlan-

tic Treaty Organization (NATO) could face a tactical nuclear response, practically denying the Alliance the option to free the occupied territory with conventional military means.

In Eastern Europe, a rapid invasion in various scenarios could create a *fait accompli* attack that favors the Russians. Possible settings include the Baltic states, the Suwalki Gap to open a corridor to Kaliningrad, parts of eastern Poland, or the northern sector of Nordkapp and Svalbard as a perimeter defense of Murmansk. According to a U.S. Army publication, a “*fait accompli* attack is intended to achieve military and political objectives rapidly and then to quickly consolidate those gains so that any attempt to reverse the action by the [United States] would entail unacceptable cost and risk.”²²

The rapid *accompli* attack would likely be well planned because the attacker would have the time to prepare and identify targets and goals pivotal for reaching the desired endstate. Today’s information-rich public environment and public access to infrastructure in the potential target area enable the covert planning of an *accompli* attack with a high level of granularity and certainty regarding the physical environment in the target area. In this planning, the attacker needs to validate assumptions of future outcomes of the engagement with the defending force, as these assumptions must be true for strategic success.

The first assumption is that the United States and NATO would not be the first to use nuclear arms. Kenneth Waltz writes, “Deterrence depends on what one can do, not on what one will do.”²³ As long as the United States and the Alliance have nuclear capabilities, this assumption is a part of the equation for a potential attacker planning an *accompli* attack. Even if NATO has a declared posture not to be the first actor to use nuclear arms, it is irrelevant, as an actor could change its will and intent within a fraction of a second. It cannot ignore the presence of nuclear capabilities.

The second assumption is that the movement of larger U.S. and NATO forces to the theater will take more

time than the Russian advancement. Depending on the scenario, the time for ground force formations to arrive from Western Europe and the continental United States could be several weeks after factoring in uncertainty for readiness, activation, and capacity.⁴ Recent joint NATO and U.S. exercises such as Trident Juncture 2018 have shown the complexity and time expenditure of moving large formations across Europe. These movements are preplanned and in peacetime. In a conflict, the sea port of debarkation (SPOD) and aerial port of debarkation (APOD) can be assumed to be under attack from standoff weaponry and hypersonic missiles. Even if U.S. and British forces arrived in the Netherlands, Belgium, and Germany, eastern Poland is still 800 miles farther east, equal to the distance between Chicago and New York City. Also, there are three major river crossings: the Elbe, the Oder, and the Vistula. In a darker scenario, disruptions through cyber effects and infrastructure sabotage have occurred already, as units seek to leave home bases toward ports of embarkation.

The estimates for the arrival of major U.S. forces to the theater depend on variables that are hard to quantify with certainty, but we assess it to be several weeks. Partial air assets, smaller formations, and U.S. forces already in Europe will arrive sooner. The European NATO countries are likely not activating and mobilizing their main unit formations until the *accompli* attack is under way. The NATO fixed command and control facilities are likely targeted in the initial hours of the *accompli* attack by Russian ballistic, cruise, and hypersonic weapons. This will lead to increased confusion and disruption and will lay a foundation for Russian information dominance. These factors add to the concern over the length of time needed for friendly units to arrive in theater.

During the past year, U.S. lawmakers have raised concerns about the readiness and capacity of military sealift.⁵ For an adversarial planner of an *accompli* attack, this time lapse until major forces arrive in the theater represents a window of opportunity. Even if Russia is strategically

inferior to the United States and NATO, the rapid *accompli* attack expects to face resistance from only a fraction of U.S. and NATO forces during its short execution.

The third assumption is that the Russians can break up the joint forces and disallow multidomain operations limiting the fighting abilities of the present ground force. The fourth assumption is that the adversary’s advantage in electronic warfare can neutralize U.S. and NATO forces’ ability to communicate, leading to the adversary’s information supremacy. Indirectly, if the fourth assumption is valid, the third assumption is then validated because the electronic attack on satellite communications and line-of-sight (LOS) tactical radio would deny joint operations and the utilization of air strikes and standoff weaponry. In a future peer conflict, a strategic surprise by the loss of ability to communicate due to electronic warfare is a tangible threat that could break up joint forces, disallow multidomain operations, and paralyze the defender; meanwhile, the adversary will advance with momentum and force.

Senior Army leadership presented the change in the strategic and tactical environment in an email to the force: “Many of the conditions we have grown accustomed to over the past eighteen years will not exist in future battles. Control of the air will be contested; Forward Operating Bases will not provide a safe haven; units will be continuously targeted by enemy fires; and communications and navigation systems will be intermittent at best.”⁶

For a potential future conflict with capable near-peer adversaries such as Russia, it is notable that they have heavily invested in the ability to conduct electronic warfare (EW) throughout their force structure. During the Cold War, the Soviets advanced electronic warfare and used both active EW and passive means in the electromagnetic spectrum (such as direction finding and signals intelligence).⁷ The Russians benefit from decades of uninterrupted prioritization and development of EW. Skills and techniques inherited from the Soviet Red Army are today the foundation for Russian ground force EW doctrine. The

Russian integration ranges from a company-size EW unit at the brigade level, a battalion-size EW unit in the Russian combined arms army, to an EW brigade in the military district.⁸

In the early days of a conflict in Eastern Europe when the primary U.S. and allied EW assets are still in Western Europe and the continental United States, the Russians would likely have a first-mover advantage and would be seeking information supremacy by denying and degrading the defending forces' communications. In a future peer conflict, a strategic surprise by the loss of the ability to communicate due to electronic warfare is a lethal threat. The Russians are not alone in upgrading their EW abilities. Several potential peer and near-peer adversaries are increasing their efforts to counter U.S. forces by denial of the radio spectrum through jamming and other EW efforts. Especially vulnerable are satellite communications (SATCOM), very high-frequency (VHF), and ultra high-frequency (UHF) line-of-sight communications, all of which U.S. forces depend on in the multidomain fight. The U.S. and NATO forces have had limited experience with EW against tactical communications since the end of the Cold War three decades ago and almost two decades of counterinsurgency operations. During these recent decades, U.S. and NATO forces have experienced undisrupted VHF, UHF, and SATCOM. These communication modes provide reliable high-bandwidth communications allowing streaming video and high-volume data transfers. Friendly forces cannot assume that there will be undisrupted communication and bandwidth in the future; the adversary will exploit and take advantage of a single point of failure found in the friendly force use of only LOS communication channels.

The Initial Conflict

Hostile electronic warfare elements deployed within theaters of operation threaten to degrade, disrupt, or deny VHF, UHF, and SATCOM. In this scenario, high-frequency (HF) radio is a viable backup mode of communication. HF radio systems have limited band-

width that does not allow streaming video, massive data flows, and larger files to be shared. However, it has a capacity sufficient to transfer short messages and support command of the ongoing fight.

The focus in recent years has been on Russian hybrid warfare and special forces, but if there is a future peer-to-peer conflict with Russia, the main encounter will be with the core of the Russian army: the infantry and armor. The Russian army focuses on an offensive posture favoring an intensive and aggressive initial stance in the early stages of a conventional conflict.⁹ The Russian army has inherited a legacy from the Soviet Union, where electronic warfare is an integrated part of maintaining speed in the offensive.¹⁰ It enables forward-maneuver battalions to engage and create disruption for the enemy and an opportunity for exploitation.

Russian Doctrine and Inherited Soviet Offensive Tactics

The Russian EW tradition goes deep. In the early days of the Soviet Union, the Communist leadership focused on hard science, equating science with progress. Science, in combination with ideology, would lead the way to the utopian society that the Communists envisioned. Once they took ownership of the means of production and the riches of Russia, science would enable a more prosperous and better life. Science was knowledge, and in the hands of the working class it became an alternative to religion. This also led to advances in math, physics, chemistry, and other natural sciences. As a result, the Soviets had advanced EW abilities in the early 1950s, and Russia has maintained the capability through the years.

Recently, Russia has executed hybrid warfare, specifically in the Donbas region of Ukraine. This action displayed a doctrine utilizing multiple attack vectors to seek information dominance. These different attacks are information operations to confuse, cyber attacks and electronic warfare to deny the adversary access to the spectrum, and direct kinetic strikes on the adversary

information infrastructure.¹¹ At a strategic level, before a conflict takes place, the Defense Intelligence Agency (DIA) notes the Russian doctrine: "Russian propaganda strives to influence, confuse, and demoralize its intended audience, often containing a mixture of true and false information to seem plausible and fit into the preexisting worldview of the intended audience."¹² The doctrine seeks to create cleavages and exploit internal tension in targeted societies as well as to weaken societal cohesion and willingness to fight. The formal Russian phrase is *information confrontation*, which utilizes all means to gain an advantage over another state by using information as a vehicle, and this concept is both technical and psychological.¹³

The psychological goal is to influence adversary beliefs, perceptions, choices, preferences, and decisions, and serves as a psychological weapon, following the heritage of the Soviet propaganda apparatus. This information manipulation is often termed "perception management," which is focused on how the target perceives reality and its options instead of its perception of Russian abilities.¹⁴

The Russian doctrine seeks dominance as early as possible in a conflict, during the initial period of war.¹⁵ When Russian strategic leaders assess that conflict is imminent (and in the accomplishment of the attack, they are the first to know), the initial stage is entered with the goal of reaching information dominance to support the speed and mobility of contemporary operations. The force is designed to be offensive and to seek dominance early in the conflict, creating early stage opportunities for exploitation by splitting NATO multinational and joint operations through denial-of-spectrum access. Information dominance becomes the nonnuclear way to break through U.S. and NATO defenses. Vladimir Slipchenko, the Russian general and influential military thinker, wrote that "superiority over an opponent was only possible after superiority in information, mobility, and rapidity of reaction were assured."¹⁶

Earlier, the Soviet offensive doctrine emphasized the use of tactical nuclear



Soldiers with Enhanced Forward Presence Battle Group Poland arrive in Rukla, Lithuania, after 2-day tactical road march across Eastern Europe, June 18, 2017, as part of exercise Saber Strike 17 (U.S. Army/Justin Geiger)

weapons to maintain momentum and thrust in the assault: “Nuclear strikes do not represent some kind of isolated act, but a component of combat. The operations of tanks and motorized rifle units are closely coordinated with them. Nuclear strikes and troop operations represent a uniform and inseparable process joined by a common concept.”¹⁷

In the Soviet-Russian army from the 1960s and forward, the basic building block of the order of battle has been the motorized rifle regiment, and the dominant tactical stance is offensive.¹⁸ A DIA publication titled *The Soviet Motorized Rifle Battalion* includes a short introduction to Soviet doctrine:

*Soviets stress the decisive nature of the offensive and emphasize the meeting engagement more than any other type of offensive action. High rates of advance are anticipated from the actions of combined arms units operating in conjunction with airborne, airmobile, and special operations forces in the enemy rear area.*¹⁹

The same publication describes combined arms:

The Soviets identify three types of combat action—the meeting engagement, the offense, and the defense. The offense is further subdivided into the attack and its exploitation, and pursuit is culminating in encirclement. The offensive is conducted by maximizing maneuver, firepower, and shock action.

The Russian doctrine favors rapid employment of nonlethal effects, such as electronic warfare, to paralyze and disrupt the enemy in the early hours of conflict.²⁰ The Russian army inherited the legacy of the Soviet Union and its integrated use of EW as a component of a greater campaign plan, enabling freedom of maneuver for combat forces. The backbone of Russian doctrine for maneuver warfare tactics has remained almost intact since the Cold War. The rear echelons are postured to utilize either a single envelopment, to attack

the defending enemy from the rear, or a double envelopment, to destroy the main enemy forces by unleashing the reserves. Ideally, a Russian motorized rifle regiment’s advanced guard battalion makes contact with the enemy and quickly engages on a broader front, identifying weaknesses permitting the regiment’s rear echelons to conduct flanking operations. These maneuvers, followed by another motorized regiment flanking, produces a double envelopment and destroys the defending forces.

The Russian formation is likely to seize and retain as much ground as possible before the enemy can react—producing either a decisive victory or a prolonged low-intensity conflict. Russian forces need an advantage that paralyzes NATO and U.S. troops. In World War II, the overwhelming massed artillery fire that fixed or destroyed the enemy paved the way for the advancement of forces. During the Cold War, tactical nuclear munitions were intended to paralyze and disperse the NATO defenses.

In the coming decade, it is highly plausible that the Russians could execute an already prepared preconflict EW blitz, seeking information dominance that degrades or denies VHF, UHF, and SATCOM. When these communication modes are degraded, having the ability to use HF communication will enhance the U.S. and NATO ability to communicate.

Reliance on LOS Communications

After two decades with uncontested spectrum, the Armed Forces are used to having available bandwidth, communications, and ability to switch between communication channels with limited interruption and excellent quality. Counterinsurgency operations have provided rear operational areas with a stable energy supply, the ability to set up satellite and radio links, and stable communication channels to higher commands, air assets, medical resources, and the logistics chain. Our potential near-peer adversaries are fully aware of our dependence on these communications channels and how their loss would impact the U.S. way of warfighting. Satellite communications are especially vulnerable for several reasons. First, the satellites transmit at lower power levels, making them easier to jam. Second, weather and space weather (solar flares) can negatively impact satellite communications. Third, the compact and fragile design of satellites themselves makes them subject to failure due to space debris or potentially an attack from an adversary's satellite. Finally, the satellites can be difficult to upgrade and could, over time, be vulnerable to cyber attacks.²¹

Former Deputy Secretary of Defense William J. Lynn III noted that

the willingness of states to interfere with satellites in orbit has serious implications for our national security. Space systems enable our modern way of war. They allow our warfighters to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity. Without them, many of our most important military advantages evaporate.²²

Avoiding Strategic Surprise

The Russian investment in EW capabilities is significant, and EW units are organic to any Russian formation from the brigade combat team and higher. This can provide a significant strategic advantage in the early stage of a conflict. The Russian formations can already engage cyber and electromagnetic effects in the initial period of war.

U.S. and allied ground forces could offset initial strategic inferiority with airpower, naval power, and global strike capabilities, but doing so depends on communication channels between ground forces and joint assets. The focus of the adversary's electronic warfare is to deny U.S. communications. One alternative is to retrograde and utilize HF communications, which was the communication channel of World War II and the Korean War. HF radio waves propagate by bouncing off the ionosphere, allowing for beyond-LOS communications. Due to the skywave propagation pattern, it is more difficult for the enemy to perform spectrum denial. Also, modern digital transmission modes allow for communications to occur at low power levels, complicating adversary detection.

The Army's ability to employ HF radio systems has atrophied significantly since the Cold War, as the United States transitioned to counterinsurgency operations. Meanwhile, the Air Force and Navy have maintained a fundamental ability. Alarmingly, as hostile near-peer adversaries reemerge, it is necessary to reestablish HF alternatives should VHF, UHF, or SATCOM come under attack and be lost as viable options for battlefield communications. HF communication has its inherent weaknesses and challenges, but they do not negate the fact that it can provide communications beyond the line of sight, which can serve as an alternative in critical junctures. By stepping back and being able to retrograde to HF as a resiliency measure, the United States is increasing communication redundancy. This also adds an asymmetric advantage when the adversary has to divert EW assets with a different set of requirements to address the HF ability, which requires more resources to disrupt and degrade.

The HF propagation patterns would send signals to broader areas, which allows the adversary to hear the signal and direct countermeasures, but it also will enable parts of the propagation to pass through sufficiently to get communication established even in a highly saturated EW environment.

HF jamming equipment requires more energy and has a significant signature, which enables U.S. and NATO neutralizing attacks with standoff weaponry and anti-radiation missiles to be successful. The Russian armed forces utilize HF communications as well, and a broad and unrestricted HF jamming can degrade and disrupt their own communications. There is also a possibility that the HF transmission propagates in a way that cannot be heard by the adversary, providing an undisrupted communication. On the other hand, LOS communications have a more narrow propagation channel, which allows the EW attacker higher certainty that communications are denied or degraded.

All the branches have limited competency with HF radio systems; however, there is a strong case to train and ensure readiness for the utilization of HF communication. Even in electromagnetic spectrum (EMS)-denied environments, HF radios can provide stable, beyond-LOS communication, permitting the ability to initiate a prompt global strike. While HF radio equipment is also vulnerable to electronic attack, it can be difficult to target when configured to use near-vertical incident skywave (NVIS) signal propagation. This high-angle take-off propagation method provides the ability to refract signals off the ionosphere in an EMS-contested environment, establishing communications beyond the line of sight out to 400 miles. Due to the high-angle signal path, the ability to direction find and target an HF transmitter is more complicated than transmissions from VHF and UHF radios that transmit LOS ground waves. Also, Russian listening posts located outside of the 400-mile radius cannot intercept the communications. The recent digital modes utilizing 3G Automatic Link Establishment (ALE) technology allow for



Soldiers from 173rd Airborne Brigade prepare for Joint Warfighting Assessment 18 in Grafenwoehr, Germany, April 2018 (U.S. Army/John Hall)

digital communication at lower power levels than what was previously required for voice. This technology allows for tac chat messaging along with digital voice within a 3G ALE network. Using lower power is a crucial advantage when trying to prevent direction finding, and adding encryption to the digital signal helps prevent signal interception. These are low-cost opportunities for the United States to increase unit survivability and battlefield effectiveness by achieving a stealthier communication channel that potential adversaries will have difficulty locating.

The expense to attain an improved HF-readiness level is low compared to other Department of Defense initiatives, yet the return on investment is high. The equipment (Harris AN/PRC-150) has already been fielded to maneuver units. The next step is leaders prioritizing soldier training and employment of the equipment in tactical environments, linking to HF networks, and integrating the HF networks into the joint force.

After almost three decades of limited interest for ground force HF communications, there are knowledge gaps to fill to ensure the optimal tactics, techniques, and procedures. Science and technology have advanced during these decades; therefore, there are multiple opportunities to cost-effectively enhance and improve the HF communication ability, especially pushing targeting data through HF communications. The revival of HF communications as a resilience measure will posture the joint force in a state of higher readiness for future conflicts.

Recommendations

We propose five activities that would rapidly improve joint force and NATO ability to utilize HF as an alternative communication channel in the future fight.

First, each branch of the joint force must train on the equipment already fielded with the focus on establishing communication in an EW-saturated environment. The HF equipment is

seldom properly used or connected in an HF network.²³ The equipment is in many cases assembled and tested to see if it transmits but is not integrated into the exercises as a fallback when other ways of communications fail. All branches of the Armed Forces have through the years acquired significant knowledge about how to use HF, but since the end of the Cold War, the understanding and experience are no longer shared on a large scale. An instrumental path to success in an HF training program is understanding HF antenna configurations. Since HF is a beyond-LOS communication channel, operators must understand how to optimize antenna arrangements depending on where they intend to propagate their signal. These skill sets are in many cases today almost nonexistent, even if the unit has fielded HF equipment and needs to be trained. This training can be supported by online training, applications that provide guidance for directions, antenna configuration, optimal transmission



Space and Missile Systems Center's Wideband Global SATCOM-10 encapsulated satellite, mated with Delta IV launch vehicle, stands ready for launch at Cape Canaveral Air Force Station, Florida, March 15, 2019 (Space and Missile Systems Center/Van Ha)

power, and advice on how to create ad hoc antennas. The ability to communicate using HF within the joint force and with NATO requires that each branch first and foremost can communicate within itself.

Second, a revised joint spectrum management effort within U.S. European Command and other unified combatant commands is necessary to ensure optimal usage of a limited spectrum. The HF range provides NVIS, which creates propagation patterns that cover 300 miles and would serve a theater. The increased HF range compared to tactical LOS communication requires predefined spectrum management.

Third, HF communication must be injected as a part of the operations in joint and multinational exercises. The East European NATO armies have upheld an HF capacity since the Cold War. In an accomplished scenario, the ground forces that are engaged in the initial fight are Baltic, Polish, and East European

forces. For these forces, HF is an integrated part of their communications, and the ability to fight as a unified NATO force is strengthened by a coherent ability to use HF communications. Joint and multinational exercises should include HF training and maintenance and the ability to relay messages, create simple HF networks, and transfer tactical and operational data through them. The HF networks' ability to transfer data is limited, but orders, directions, calls for fire, and updates can be text messages that parsimoniously use bandwidth.

Fourth, HF capacity, once seen as obsolete and replaced by VHF/UHF, has been removed to free up space and lower weight in several fixed-wing, helicopter, and vehicle assets. In some cases, versions of a particular platform can differ in the ability to communicate using HF where the older version has the HF ability as delivered from the factory in the 1990s while the updated version has had HF radios removed. This requires retrofitting

HF ability back into the platform. Each branch of the Armed Forces needs to add, modify, and update the HF capacity, even if the equipment is fielded to fighting formations and the ability across the branches is fragmented and not uniform.

Fifth, in our view, the ability to connect the fight on the ground to joint and NATO strike abilities is pivotal to delay, disrupt, and destroy Russian progress in an accomplished attack and slow down the advance until major NATO formations arrive. Joint Terminal Attack Controllers (JTACs) and their NATO equivalent, affected by adversarial electronic warfare, are of no operational value if they cannot communicate the targeting information. The rapid injection of JTAC ability across the theater, even in the territorial forces of our East European allies (such as the Polish Territorial Defence Force, which uses HF to communicate), brings the strike abilities of the joint force to NATO forces on the perimeter that risk being overrun by a rapid Russian advancement.



Mechanized infantry battalion 45 Painbat, Regiment Infanterie Oranje Gelderland, Royal Netherlands army, during cold weather training as part of NATO's exercise Trident Juncture 2018, Norway, October 2018 (Courtesy NATO/The Netherlands/Hille Hillinga)

As General Mark Milley stated, “Units will be continuously targeted by enemy fires; and communications and navigation systems will be intermittent at best.”²⁴ In a combat environment where communication systems will be intermittent, we have sought alternative solutions to ensure that the JTAC communication goes through even if SATCOM and VHT/UHF fails, where theater-wide HF NVIS was presented as an alternative route. If HF NVIS fails, the Military Auxiliary Radio System (MARS) could fill a new modern role where JTAC and other tactical information using other than NVIS frequencies propagates out of theater and is received by MARS, which relays the information to the appropriate receiver. The approach is nontraditional, but numerous MARS-enrolled radio amateurs comprise a highly knowledgeable asset in HF communication. Our fifth recommendation is to draw attention to the complexity and necessity to link JTACs to the joint force facing an accomplished attack that rapidly unfolds.

Conclusion

U.S. and Alliance deterrence on the eastern NATO border has several components that depend on each other in the calibrated force posture against Russian aggression and attack. One identified concern is the Russian ability to quickly launch an accomplished attack with limited or no early warning. An accomplished surprise attack is a rapid move, with little preparation and forewarning, to establish a fait accompli and to radically strengthen the adversary’s bargaining position.

If Russia launches a fait accompli attack in Eastern Europe, the arrival of sizeable U.S. and NATO forces in the theater is likely weeks away. If APOD, SPOD, and transportation infrastructure within Western Europe is under attack, the attacker has additional time, as these attacks will cause delays for the NATO forces. The risk is that it is enough time to establish a fait accompli territorial gain with limited resistance against the invading force.

A pivotal part in the Russian calculation is the ability to separate joint operations and disallow defending ground forces access to airpower and standoff weaponry. A key component in achieving separation of joint forces is electronic warfare and the disruption and denial of U.S. and NATO communications.

The U.S.-NATO ability to maintain communications that hinder a split of joint operations, even at less quality, bandwidth, and reliability, creates uncertainty for the potential attacker. Our NATO allies, especially the Eastern European countries, still maintain an HF communication infrastructure. With limited investments in time and personnel and using existing fielded equipment, U.S. forces can strengthen the communication and information resiliency against massive hostile EW activities. An enhanced U.S. ability to communicate by HF radio would strengthen the ability to conduct joint operations, as

New from NDU Press

for the Center for Strategic Research

Strategic Forum 304

Baltics Left of Bang: Nordic Total Defense and Implications for the Baltics Sea Region

By Håkon Lunde Saxi, Bengt Sundelius, and Brett Swaney



The efforts of Norway, Sweden, and Finland to enhance societal resilience through unique “total defense”

and “comprehensive security” initiatives are unlikely to change the near-term strategic calculus of Russia. Over time, however, a concerted application of total defense in harmony with Article 3 of the North Atlantic Treaty will aid in the resilience to, and deterrence of, Russian hostile measures and hybrid warfare, and serve as a complement to a regional denial-based deterrence strategy. The Nordic states could “export” resilience to the greater Baltic Sea Region by strengthening participation in European Union energy and infrastructure projects with the Baltic states, amplifying efforts to connect infrastructure links among allies and partners and decouple from adversaries.

communications could relay through NATO allies to the U.S. joint force.

The risk that a small and outnumbered U.S.-NATO ground force can sufficiently communicate through an EW-saturated environment to link up with the joint force represents a single point of failure for any Russian fait accompli attack planning. The U.S. ability to retrograde and use HF communications creates an uncertainty hard for any Russian war planner to quantify and grasp as a potential risk for operational failure of a fait accompli attack. HF radio communication is not a perfect alternative to SATCOM and VHF/UHF line-of-sight communications, but it is an option that is tangible, fielded, and can cost-effectively increase both abilities and regional deterrence. From a U.S. perspective, the fear is that it might not work. From a Russian perspective, the concern is that it might work. Uncertainty is by itself a deterrent. JFQ

Notes

¹ Department of Defense, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, 2016).

² U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, December 6, 2018).

³ Kenneth N. Waltz, “Nuclear Myths and Political Realities,” *American Political Science Review* 84, no. 3 (September 1990), 733.

⁴ Mahyar A. Amouzegar, “Military Logistics,” in *Routledge Handbook of Defence Studies*, ed. David J. Galbreath and John R. Deni (Abingdon-on-Thames, UK: Routledge, 2018), 113.

⁵ Geoff Zieczulewicz, “Lawmakers Express Concerns over Navy’s Aging Surge Sealift Fleet,” *Navy Times*, March 9, 2018, available at <www.navytimes.com/news/your-navy/2018/03/09/lawmakers-express-concerns-over-navys-agings-sealift-fleet/>.

⁶ Daniel A. Dailey, Mark A. Milley, and Mark T. Esper, “Army Senior Leaders Send—Lessons from D-Day,” *Army.mil*, June 6, 2019, available at <<https://home.army.mil/stewart/index.php/about/news/army-senior-leaders-send-lessons-d-day>>.

⁷ *Threat Handbook: Battlefield Survival and Radioelectronic Combat* (Fort Monroe, VA: TRADOC, February 1983).

⁸ Roger N. McDermott, *Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electro-Magnetic Spectrum* (Tallinn, Estonia: International Centre for Defence and Security, September 2017).

⁹ Valeriy Gerasimov, “The World on the Verge of War” [Mir na granyakh voyny], *Military Industrial Courier* [Voyenno-promyshlenny kuryer], March 15, 2017, available at <<http://vpk-news.ru/articles/35591>>; Aleksandr V. Rogovoy and Keir Giles, *A Russian View on Land Power*, The Letort Papers (Carlisle Barracks, PA: U.S. Army War College Press, April 2015).

¹⁰ *Russian Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017).

¹¹ T.S. Allen and A.J. Moore, “Victory without Casualties: Russia’s Information Operations,” *Parameters* 48, no. 1 (Spring 2018), 59–71.

¹² *Russian Military Power*, 38.

¹³ Olga Filatova and Radomir Bolgov, “Strategic Communication in the Context of Modern Information Confrontation: EU and NATO vs. Russia and ISIS,” in *Proceedings of the 13th International Conference on Cyber Warfare and Security*, ed. Jim Q. Chen and John S. Hurley (Washington, DC: ACPIL, 2018), 208–219.

¹⁴ Timothy L. Thomas, “Deterring Information Warfare: A New Strategic Challenge,” *Parameters* 26, no. 4 (Winter 1996–1997), 81.

¹⁵ Timothy L. Thomas, “Russian Forecasts of Future War,” *Military Review* (May–June 2019).

¹⁶ Ibid., 88.

¹⁷ Andrei Alekseevich Sidorenko, *The Offensive (A Soviet View)* (Washington, DC: U.S. Government Printing Office, 1973).

¹⁸ Frederick R. Wilson, *United States Perceptions of Soviet Tactics versus Contemporary Soviet Tactical Writings* (New York: U.S. Army Russian Institute, 1979).

¹⁹ Robert M. Frasche, *The Soviet Motorized Rifle Battalion*, DDB-1100-197-78 (Washington, DC: Defense Intelligence Agency, 1978).

²⁰ V.I. Kuznetsov, Yu.Ye. Donskov, and A.S. Korobeynikov, “Electronic Warfare and Information Warfare: How They Compare,” *Military Thought* 22, no. 1 (2013).

²¹ Jan Kallberg, “Designer Satellite Collisions from Covert Cyber War,” *Strategic Studies Quarterly* 6, no. 1 (2012), 124–136.

²² William J. Lynn, III, “A Military Strategy for the New Space Environment,” *The Washington Quarterly* 34, no. 3 (2011), 7–16.

²³ Robert L. Edmonson et al., “Tactical Employment Considerations of HF Radios in the Cavalry Squadron,” *The Cyber Defense Review* 4, no. 1 (Spring 2019), 23–32, available at <www.jstor.org/stable/26623064>.

²⁴ Dailey, Milley, and Esper, “Army Senior Leaders Send—Lessons from D-Day.”



Visit the NDU Press Web site for more information on publications at ndupress.ndu.edu



Chief Master Sergeant Darin LaCour, 149th Fighter Wing command chief, speaks to enlisted Airmen of importance of professional military education, at Joint Base San Antonio–Lackland, Texas, November 2, 2019 (Air National Guard/Derek Davis)

Strategic Leader Research

Answering the Call

By Larry D. Miller and Laura A. Wackwitz

Senior Service colleges (SSCs), as premier providers of joint professional military education (JPME), are well positioned to produce the range of thought and scholarship required to sustain national security during uncertain times. JPME nevertheless struggles to meet the needs and expectations of the two primary audiences for senior

leader research: professional military and academic civilian. All too often, efforts to advance strategic thought are hampered by this conflict of constituencies.¹ Yet centering strategic leader research and writing within JPME could make possible the bridging of these worlds to establish SSCs as innovative centers capable of marshalling warrior experi-

ence while inspiring intellectual creativity. With students and faculty as active participants in problem-solving and idea generation, SSCs can establish a culture wherein ideas are valued for their ability to positively impact both policy and the larger strategic community. From the position of strength engendered by producing senior leaders able to communicate innovative ideas, SSCs will not only address the criticisms leveled against JPME, but they will also sharpen the cutting edge of strategic progress.

Dr. Larry D. Miller is Research Professor of Communicative Arts and an Editor with the U.S. Army War College Press. Dr. Laura A. Wackwitz is the Director of the Institute of Military Writing.

A Conflict of Constituencies

SSCs are populated by military professionals, many of whom have modest preparation and reluctant motivation for rigorous engagement with graduate-level education. Most officers are selected to attend by virtue of prior accomplishments and future promise with little regard for academic preparation. Tapped from within a system in which “traditional military skills are rightly valued . . . but cognitive skills are largely dismissed,”² matriculating officers are mature, highly experienced, and professionally accomplished, yet their facility with the conventional tools of graduate education may be lacking. Thus, entering classes do not necessarily have consistency among students to successfully employ the techniques of close reading, careful research, critical thinking, and effective writing.

Because of these challenges, some proponents of JPME maintain that “ivory tower” tools are overrated; writing and research will neither build nor defend the Nation’s house.³ Other proponents completely eschew pursuing schoolhouse inquiries of any kind. Too much thought, as one extremist argues, “clouds a senior officer’s judgment, inhibits his instincts, and slows his decision-making.”⁴ The most vehement critics, on the other hand, believe that neither SSC students nor JPME institutions measure up. To them, “no admission standards plus no selectivity (a term civilian universities use) equals remedial education.”⁵ The logical extension of that argument is to simply disband, dismember, or reconfigure SSCs, as some have suggested.⁶ So what is the solution?

At first glance, the situation appears untenable: one institution, or even a group of institutions, cannot possibly satisfy two disparate camps anchored by extreme positions. History supports this conclusion. But the importance of the mission must supersede the impulse to continue the practice of dodging professional bullets with academic arguments and academic bullets with professional ones. Though traditional academics and most professionals involved with JPME would argue that thoughtful inquiry

enhances judgment, refines instincts, and improves decisionmaking, opinion is divided regarding the vitality of JPME as a vehicle for inspiring the habits of mind required to thoughtfully engage complex materials.⁷

From a JPME perspective, SSCs are professional military institutions, and as such each schoolhouse requirement constitutes a task to be negotiated or tolerated en route to higher levels of responsibility. The impulse is high for faculty to satisfy both senior leadership and student expectations by delivering instruction as systematically, efficiently, and conveniently as possible. Because SSC students are successful, well-paid military professionals, the operant mentality is that if research is necessary, topics to be addressed should be of particular importance to senior leadership. Lists of topics, issues, and questions provide a smorgasbord of opportunities to align research efforts with a specific concern or tasking.⁸ When asked to conduct research, students are to select a strategic issue, analyze extant information, and offer recommendations in writing to one or more designated points of contact (POCs)—possibly even in the absence of high-quality analysis essential to actionable recommendations.

From an academic perspective, SSCs are professional military institutions granting accredited graduate degrees funded by the American public and, as such, should step up to the intellectual plate. Viewed as public servants, SSC students have a golden opportunity to expand their capabilities while contributing to national security—an opportunity not available to the majority of the population. Consequently, those who fail to make the most of that opportunity are regarded as little more than well-paid freeloaders and exploiters of the public trust. Military emphasis on “training” and “guidance” alienates most academicians who view education as a progressively unfolding inquiry requiring guided exploration more than authoritarian direction. To academics, lists at the graduate level should be reading lists, not topic lists. POCs should be between experience and ideas, practice

and theory, not people and offices. Senior Service colleges, therefore, are readily criticized for lack of rigor,⁹ subordination of intellectual opportunity, minimization if not rejection of genuine inquiry, and questionable commitment to academic freedom.

A more integrated approach is in order—one that challenges conventional wisdom on both sides without succumbing to Derridean-style deconstruction. By capitalizing on the talent and strengths at hand, JPME can effectively maneuver away from the box into which it has been placed. Embracing a 21st-century education requires SSCs to directly engage students in meaningful explorations of complex ideas made clear through research and writing. This must be accomplished with the understanding that in an academic world populated by accomplished military professionals, word-one is not square-one, and success is measured not primarily by rank or the next assignment but by contributions.

Harnessing the Power of JPME

The opportunity for JPME to embrace the development of warrior-scholars comes at a time when the uncertainty of the future has given way to the uncertainty of now.¹⁰ Senior U.S. military leadership continues to lack consistent abilities to connect war to policy in ways that impact the national strategic posture.¹¹ Information absent analysis and thoughtful interpretation is of little use to those charged with protecting our citizens, maintaining our sovereignty, and advancing national interests. Warrior-scholars can bridge the information-interpretation gap only if SSCs better educate students to utilize research, writing, critical thinking, logic, and reason to develop, implement, and/or recommend responsive strategic options to dynamic national security issues. This requires a fundamental shift in perspective among JPME institutions and the commitment to engage in an unprecedented embrace of research and writing as essential leader capabilities and valued forms of national service.¹²

Today’s senior military officers are some of the most experienced and



Marine with Headquarters Battalion, 3rd Marine Division, talks about World War II beach landing on Iwo Jima during professional military education brief, Iwo Jima, Japan, November 26, 2019 (U.S Marine Corps/Esgar Rojas)

knowledgeable advocates for national security in the history of the United States, yet SSCs consistently fail to bring student expertise to the fore, opting instead to serve as networking centers for career professionals with a soft introduction to strategy on the side (faculty efforts to stimulate intellectual growth notwithstanding). To better facilitate the development of an effective future force built on the ideas and insights of JPME's rising strategic leaders, SSCs must combine the best of two worlds to unite academic inquiry and skill sets with highly experienced military professionals invested in our national future.

As General Martin Dempsey, USA (Ret.), former Chairman of the Joint Chiefs of Staff, observed, the call to arms and the quest for knowledge are united through individual and collective effort: "Every member of the force should seek to be a scholar of the Profession of

Arms in their own right and a teacher to those coming along behind."¹³ Rather than allowing JPME to remain lost in the quagmire of the civilian-academic versus professional-military critique, faculty, students, and administration must together embrace a better, more sustainable reality—one in which the combined knowledge of JPME students and SSC graduates can be communicated effectively by warriors equipped and inspired to become scholars well armed with ideas, information, and the transformative power of words.¹⁴

Although the steps to a successful transformation could take many forms, four are recommended here. First, abandon the mindset that writing is and should remain the province of the intellectual elite, Ivy League-educated academics, professional researchers, and think tank scholars. Though some have argued that JPME develops leaders,

not researchers, strategists, not writers,¹⁵ the importance of effective written communication cannot be understated. Without quality writing and attendant critical thought, knowledge and valuable experience are lost. Without research and perceptive interpretation of experience, insight is debilitated. JPME must, therefore, recognize all SSC students—regardless of their prior writing experiences—as scholars in the making, individuals whose potential and promise for the future must not be overlooked or left undeveloped. SSCs routinely cultivate the abilities of senior leaders to respond to evolving conditions, employ critical thinking skills, and exercise solid judgment through sound leadership. The logical, indeed appropriate, extension of those activities is to simultaneously develop student research and writing skills such that they will be better able to manage, if not solve, strategic challenges. If,

as Charles Murray has argued, the “process of writing is the dominant source of intellectual creativity,”¹⁶ it invariably contributes to the types of “refined thinking” so often sought from strategic leaders.¹⁷ As John T. Gage argues:

*Writing is thinking-made-tangible, thinking that can be examined because it is “on the page” and not all “in the head,” invisibly floating around. Writing is thinking that can be stopped and tinkered with. It is a way of making thought hold still long enough to examine its structures, its possibilities, its flaws. The road to a clearer understanding of one’s own thoughts is travelled on paper. It is through the attempt to find words for ourselves, and to find patterns for ourselves in which to express related ideas, that we often come to discover exactly what we think.*¹⁸

Warriors who rise to the level of senior leaders, whether they realize it or not, are in many ways well primed for thoughtful scholarship. They are experienced at gathering information, assessing sources, advocating informed choices, considering arguments, making decisions, and transforming words into actions. Their training, education, and field experiences, however, do not routinely involve close engagement with the conventional tools for developing reasoned discourse: library research, critical reading, argument construction, and professional writing. JPME must fill the gap by abandoning the “good to go, keep the troops moving” mentality wherein the expectation for original thought is reserved for elite students, while others are permitted to advance with marginal competencies routinely associated with parroting existing ideas, tweaking stock point papers, and crafting visually impressive PowerPoint briefings. Long-term gain must not be sacrificed for short-term convenience and institutional expedience.

Second, integrate research and writing across the curriculum and steadfastly refuse to allow SSC students to bypass the hard work of learning to research important issues and pen effective documents. JPME cannot continue to be defined either by officers who “treat ‘schooling’ as

something distinct from serving”¹⁹ or by the presumption that military professionals are properly committed to action, not contemplation.²⁰ For many students and faculty alike, the idea persists that subject matter expertise earned through experience, untiring effort, and often grueling service should excuse SSC students from becoming effective communicators of ably researched and well-reasoned ideas. This assumption, however, could not be further from the truth. Untiring and often grueling service should entitle SSC students to the best education possible so that they may continue the path of excellence, dedicate themselves to leadership at the highest levels, and skillfully contribute to senior leader discourse as duty commands and opportunity allows.

Though SSC graduates are expected to “write well,”²¹ for many, the ability to prepare original high-quality documents that are well researched, thoughtfully analyzed, articulate, persuasive, and appropriately sourced remains elusive. Student facility with the written word, as General David Petraeus, USA (Ret.), aptly noted, may be the “one area” that PME students “need to improve across the board.”²² At first glance, the writing challenges that haunt many senior officers are a consequence of demanding professional requirements on the one hand and antecedent conditions that lie outside SSC control on the other.²³ That SSCs do not rely on conventional academic admission standards has been cited, as evidence that it may be structurally impossible to assemble what war colleges desire: a student body primed for intellectual success in a condensed graduate-level environment.²⁴ Yet this lament over admission standards serves to obfuscate the reality that, in many ways, SSCs have simply failed to provide students with the tools and inspiration to become knowledgeable, articulate, and facile with the written word. With an exceedingly low student-faculty ratio, abundant library support, qualified faculty, and an invested student body uninhibited by financial obligations, the suggestion that the majority of career military professionals—many with prior advanced degrees—cannot be taught to write at the professional graduate level

is absurd. Senior Service colleges would do well to follow the advice of Alfred M. Gray, who stated simply, “Take what you get, make it what you want.”²⁵

By adopting a developmental approach with progressively elevated expectations for written communication, JPME students can become engaged in the refined thinking necessary to respond effectively to an evolving and highly dynamic strategic landscape. Research and writing skills, like critical thinking skills, do not thrive in isolation. Their development must occur in the pursuit of strategic-level understanding, subject matter expertise, and leadership excellence. Absent perceptive faculty guidance and engaged coaching, many SSC students produce relatively uninspired research reports that, while technically satisfying institutional requirements, fall well short of delivering meaningful utility with visionary impact. The motivation to write is far greater when the task is perceived as an opportunity for communicating essential information and important ideas from an informed perspective. Mundane writing tasks that are received as little more than artificial exercises absent clear purpose and meaningful utility are unlikely to produce interesting thought, let alone good writing. Inspire the desire to communicate interesting ideas and the language to do so will follow, especially under the close guidance of committed faculty well armed with subject matter expertise. Likewise, revisioning writing as an extension of reasoning and professional knowledge will help generate a culture in which fewer faculty avoid close engagement with the ideas and linguistic competencies of their charges.

Third, stop perpetuating the false notion that in order to have something meaningful to say, colonels and lieutenant colonels must first focus on fundamental grammar and punctuation. Language mechanics are important but at this level should flow from considered ideas. Suppose, for example, that an officer has extensive experience with nuclear submarines. She wants to explore the relationship between nuclear energy and climate security but lacks linguistic



National Defense University's President's Lecture Series hosted Dr. Peter Singer, coauthor of *LikeWar: The Weaponization of Social Media*, on October 23, 2019, in Lincoln Hall auditorium (NDU/Katie Persons Lewis)

sophistication. To develop the skills and confidence to communicate her ideas effectively in writing, she does not need remediation. She needs a coach who values her ideas for what they are and helps her to find the means to express them. A shift in focus—away from SSC students' lack of academic preparation and toward their vast knowledge and ideas gained throughout a lifetime of service—provides JPME institutions with an incredible opportunity to meet students at their current skill level and help them develop ideas into written products. Traditional methodologies, however, are untenable. Nothing squashes the desire to learn new skills more fully than a corrective approach to writing or institutional reliance on numerous diagnostics (to study the problem), technological interventions (to avoid the problem), and editorial drop-off services (to fix the problem). SSCs must instead provide

sufficient opportunities for students to become confident senior leaders who use research and writing skills to generate ideas, help manage problems, and communicate effectively. Rather than simply adding more writing assignments into the preexisting mix, SSCs must foster collaborative interaction between students and faculty with meaningful feedback as the norm and warrior-scholarship as the common goal.²⁶ If guided with flexibility and grace, SSC students can themselves bridge the gap between the academic and professional military worlds by joining the community of researchers dedicated to embracing research of multiple types at all levels of investigation. It takes, in fact, all kinds of research to build understanding about all kinds of questions/topics and to meet the needs and expectations of demanding audiences. Some will write for military audiences, some for civilian; some will address professional questions,

some academic. Some questions will be directed, others chosen. All approaches can be honored and utilized for what they are and for the type of contribution they make. Full embrace of this dual role will engender institutions capable of sustaining diverse perspectives and furthering the process of inquiry in its many forms.

SSCs, therefore, must find ways to provide high-quality, JPME-specific support for emerging writers and the faculty who guide them. Writing centers must be placed front and center, well integrated into the educational mission, and supported by strategically grounded faculty who write. Though calls sound across the Services for greater written communication skills among senior officers, all too often the response is positioned near the institutional margin as an office staffed by a small cadre of competent support personnel (writing professionals and



Marines with Advanced Infantry Training Battalion, School of Infantry-East, explore Aisne-Marne American Cemetery and Memorial during professional military education trip to Belleau, Aisne, June 12, 2014 (U.S. Marine Corps/Nicholas J. Trager)

coaches).²⁷ Such offices are typically modeled as undergraduate writing centers with a largely remedial task: to spruce up fundamental writing conventions, including voice, grammar, mechanics, and punctuation. One can argue the merits of a corrective approach for college undergraduates, but not for mature college graduates who commonly hold one or more advanced degrees in addition to exceptional credentials in their professional areas of expertise.

Fourth, actively cultivate faculty investment in a revisioning writing process that encourages student-faculty collaboration. Advocating a research team mentality will enhance knowledge contributions while laying the foundation for enduring professional relationships grounded by a learner-centric environment. Networking by any other means

(for example, softball, family outings, social events) is far less effective for creating meaningful connections with subject matter relevance. By encouraging students to affiliate with faculty research initiatives, productivity will increase, knowledge will advance, and the prospect for adopting a warrior-scholar mentality will be optimized.

The congressionally mandated SSC student-faculty ratio of 3.5 to 1 affords an exceptional opportunity for student-faculty engagement.²⁸ Many faculty members work closely with students and are committed to developing student research and writing expertise. Others, however, are less invested. Just as General Robert Scales, USA (Ret.), has suggested, some students may be too busy to learn; so, too, some faculty may be too busy to teach.²⁹ Faculty who have compelling

research interests or little graduate-level teaching experience may feel overloaded by the array of activities and obligations associated with professional education at the graduate level.³⁰ Integrating faculty scholarship initiatives with student research and writing expectations can maximize time and labor efficiencies that seldom exist when working alone. As subject matter experts, faculty members are expected to maintain currency in their primary fields. Opting for a student-faculty relationship built around mentoring rather than simply “advising” will help reach this goal.³¹ With the mentor serving as an experienced guide (as opposed to primarily an arbiter of student work products), the student-mentor team can together invest in a strategic journey to explore current literature, seek connections between ideas, and develop

fresh insights. Neither the student nor the mentor should become subservient or ancillary. Students must be encouraged to find their own voices, conduct independent research, and return to the mentor for vigorous discussion about findings, controversies, and actionable ideas. A combination of genuine inquiry and close collaboration will strengthen the work product of students and faculty while simultaneously reducing academic malfeasance by those who feel isolated and/or overwhelmed by a seemingly complex milieu of unclear expectations.³² Adopting a partnership approach will support student efforts to strengthen their investigatory, analytical, and communication facility by engaging them in a process well known, understood, and valued in the military—teamwork.

Although most SSC graduates will not be expected to routinely create research documents at their next assignment, the process of having conducted research, especially within the context of a mentoring relationship, will serve them well. As Richard Kohn argues, intellectual engagement with a challenging strategic task that requires research and writing remains the “best way to prepare senior officers to recognize mistaken assumptions, inadequate research, sloppy thinking, weak analysis, imprecise writing, and unpersuasive argumentation.”³³ Research projects—when approached as an opportunity for professional development and collaborative interaction with a subject matter expert—sharpen critical thinking and articulate expression while emphasizing the role writing plays at the strategic level. Addressing these issues through apt faculty development initiatives will help empower SSCs to more fully realize their potential for becoming vibrant communities where students enter as they will and exit as well-informed strategic leaders capable of writing effectively.

The Way Ahead

The integration of research and writing skills into the professional lives of current and future senior leaders enables SSCs to better address both the needs of strategic leadership and the

conflicts of perspective that so often plague JPME. Within this construction, strategic research is at once academic and professional, military and civilian, theoretical and practical, emerging and established. The development of critical thinking, writing, and research competencies is, after all, inexorably tied to the promise of a more secure nation capable of “provid[ing] for the common defence . . . and secur[ing] the Blessings of Liberty.”³⁴ The Nation needs those being groomed for the highest levels of military leadership to transition from experienced warrior to invested warrior-scholar. One might rightly predict that our national stature and possibly our very survival in a world characterized by the “broad diffusion of all forms of power” may well depend on that transformation.³⁵ We must, as former Chairman of the Joint Chiefs of Staff General Dempsey observed in his consideration of JPME, learn to maneuver “outside our intellectual comfort zone” and “embrace change or risk irrelevance.”³⁶

In part, these goals have yet to be fully realized because they are but a smaller component of the larger task to which JPME must turn: valuing student scholarship in its own right and developing and advancing that scholarship for what it is and what it can become.³⁷ Clearly signaling to students and constituencies alike that SSCs must recognize, value, and promote high-quality student research and writing would enable JPME to solidify senior leader insights as contributory to strategic discourse. Mission command, regionally aligned forces, conflict prevention, bad actors, national disasters, humanitarian crises, and concern with the human elements of military operations all point to the importance of establishing a culture of articulate leadership that permeates the Joint Force—not one overly restricted by top-down leadership-as-usual, but revised leadership emerging from within and practiced at all levels. If JPME is to answer the call, SSCs must embrace a similar stance regarding student scholarship.

SSCs educate the best and brightest military professionals. The task now is to give voice to those studying among

us—to bring forth and encourage their candor, intellectual development, and ability to speak truth to power. SSC students have unique perspectives—borne out of experience and the simple act of seeing from different vantage points—insights that may well be overlooked by higher authority and elite think tank scholars if those perspectives are not communicated with professional elegance and persuasive clarity. JFQ

Notes

¹ For an in-depth overview of professional military education (PME) criticism, shortcomings, and challenges, see Joan Johnson-Freese, “Why War Colleges?” in *Educating America’s Military* (London: Routledge, 2013).

² Jaron Wharton et al., “Looking Beyond Professional Military Education to Evaluating Officers,” *War on the Rocks*, August 18, 2018, available at <<https://warontherocks.com/2018/08/looking-beyond-professional-military-education-to-evaluating-officers/>>.

³ Paula Thornhill, “To Produce Strategists, Focus on Staffing Senior Leaders,” *War on the Rocks*, July 20, 2018, available at <<https://warontherocks.com/2018/07/to-produce-strategists-focus-on-staffing-senior-leaders/>>.

⁴ Ralph Peters, “Learning to Lose,” *The American Interest* 2, no. 6 (July 2007), 25, available at <www.the-american-interest.com/2007/07/01/learning-to-lose/>.

⁵ Anonymous reviewer comment, *Joint Force Quarterly* e-mail message to authors, August 25, 2019.

⁶ Thomas E. Ricks, “Need Budget Cuts? We Probably Can Start by Shutting the Air War College,” *Foreign Policy*, April 11, 2011, available at <<https://foreignpolicy.com/2011/04/11/need-budget-cuts-we-probably-can-start-by-shutting-the-air-war-college/>>.

⁷ Jennifer Mittelstadt, “Too Much War, Not Enough College,” *War Room*, June 20, 2018, available at <<https://warroom.army-warcollege.edu/articles/too-much-war-not-enough-college/>>.

⁸ See *Key Strategic Issues List (KSIL) 2018–2020* (Carlisle Barracks, PA: U.S. Army War College Press, 2018), available at <<https://publications.armywarcollege.edu/pubs/3551.pdf>>. Each Service prepares and distributes a list of approved or recommended topics for research.

⁹ See Nicholas Murray, “Rigor in Joint Professional Military Education,” *War on the Rocks*, February 19, 2018, available at <<https://warontherocks.com/2016/02/rigor-in-joint-professional-military-education/>>; and James Joyner, “Professional Military Education and

the Rigor Problem,” *War on the Rocks*, March 15, 2016, available at <<https://warontherocks.com/2016/03/professional-military-education-and-the-rigor-problem/>>.

¹⁰ Joseph F. Dunford, Jr., “The Character of War and the Strategic Landscape Have Changed,” *Joint Force Quarterly* 89 (2nd Quarter 2018), 2–3.

¹¹ Richard H. Kohn, “Tarnished Brass: Is the U.S. Military Profession in Decline?” *World Affairs* 171, no. 4 (Spring 2009), 73–83, available at <www.jstor.org/stable/20671412?seq=1#metadata_info_tab_contents>.

¹² The concept “warrior-scholar” may derive from a statement commonly misattributed to Thucydides that the “nation that will insist upon drawing a broad line of demarcation between the fighting man and the thinking man is liable to find its fighting done by fools and its thinking by cowards.” The source is William F. Butler, *Charles George Gordon* (London: MacMillan and Co., 1889), 85. The idea that warriors/soldiers can or should be scholars surfaces irregularly in military writing. For example, see Scott Eflandt and Brian Reed, “Developing the Warrior-Scholar,” *Military Review* (July–August 2001), 82–89; and Robert H. Scales, “Too Busy to Learn,” *Naval Institute Proceedings* 136, no. 2 (February 2010), available at <www.usni.org/magazines/proceedings/2010-02/too-busy-learn>.

¹³ Martin E. Dempsey, *Joint Education White Paper* (Washington, DC: The Joint Staff, July 16, 2012) 5, available at <www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cjcs_wp_education.pdf?ver=2017-12-28-162044-527>.

¹⁴ Robert B. Brown commented that the “Army University will also empower students to write, debate, and improve the Army profession by actively working to publish their professional research in the broader national security dialogue. See “The Army University Educating Leaders to Win in a Complex World,” *Military Review* 95, no. 1 (July–August 2015), 27.

¹⁵ George E. Reed, “The Pen and the Sword,” *Joint Force Quarterly* 72 (1st Quarter 2014), 18, states, “War colleges are not much interested in research or scholarship.” He is not alone in that view. Nicholas Murray, writing in the same issue (“The Role of Professional Military Education in Mission Command,” 13), maintains that “teaching is the main focus of the [PME] institutions, and that should remain the case.”

¹⁶ Charles Murray, *The Curmudgeon’s Guide to Getting Ahead* (New York: Crown, 2014), 55.

¹⁷ Stephen King, *On Writing* (New York: Pocket Books, 2000), 131. For the argument that writing both directly reflects and structures thought, see Trent J. Lythgoe, “Flight Simulation for the Brain: Why Army Officers Must Write,” *Military Review* 91, no. 6 (November–December 2011), 51.

¹⁸ John T. Gage, “Why Write?” in *The Teaching of Writing*, ed. Anthony Petrosky and David Bartholomae (Chicago: University of Chicago Press, 1986), 24.

¹⁹ Kohn, “Tarnished Brass.”

²⁰ See Christopher J. Lamb and Brittany Porro, “Next Steps in Transforming Education at National Defense University,” *Joint Force Quarterly* 76 (1st Quarter 2015), 41, who comment that military culture is anti-intellectual and devalues education.

²¹ John W. Yeager, *Provost Concept for Learning and Technology Center White Paper* (Washington, DC: National Defense University, July 21, 2016), 2, available at <www.ndu.edu/Portals/59/Documents/BOV_Documents/2016/Sept/Learning%20and%20Technology%20Center%20White%20Paper.pdf?ver=2016-09-21-164304-757>.

²² David H. Petraeus, “Beyond the Cloister: Civilian Graduate Programs Broaden a Soldier’s Horizon,” *The American Interest* 2, no. 6 (July 2007), available at <www.the-american-interest.com/2007/07/01/beyond-the-cloister>. Thomas Ricks, *The Generals: American Military Command from World War II to Today* (New York: Penguin, 2012), 458, makes a similar observation: the thinking and writing skills of senior officers are deficient.

²³ U.S. Army Training and Doctrine Command Pamphlet (TRADOC) 525-8-2, *The U.S. Army Learning Concept for 2015* (Washington, DC: TRADOC, June 6, 2011), 14.

²⁴ Joan Johnson-Freese and Kevin P. Kelley, “Meaningful Metrics for Professional Military Education,” *Joint Force Quarterly* 84 (1st Quarter 2017), 67; and Joan Johnson-Freese, “Educating the U.S. Military: Is Real Change Possible?” *War on the Rocks*, May 7, 2015, available at <<https://warontherocks.com/2015/05/educating-the-u-s-military-is-real-change-possible>>.

²⁵ Alfred M. Gray, Jr., 29th Commandant, U.S. Marine Corps. See Paul Otte, comp., *Grayisms* (Arlington, VA: Potomac Institute Press, 2015), 20.

²⁶ Murray, “The Role of Professional Military Education,” 13, recommends students write regularly, possibly on a weekly basis; and Desirae Gieseman, “Effective Writing for Army Leaders,” *Military Review* 95, no. 5 (September–October 2015), 113, emphasizes the necessity for detailed feedback if writing is to improve.

²⁷ See Christopher M. Ford, “Army Leadership and the Communication Paradox,” *Military Review* 95, no. 4 (July–August 2015), 69, 72, who argues that with regard to developing communicative competence, policy and doctrine do not translate into action.

²⁸ Chairman of the Joint Chiefs of Staff Instruction 1800.01E, *Officer Professional Military Education Policy* (Washington, DC: The Joint Staff, May 29, 2015), B-4, para. (4), available at <www.jcs.mil/Portals/36/Documents/Doctrine/education/cjcsi1800_01e>.

pdf?ver=2017-12-29-142206-877>. The lowest student-faculty ratio among liberal arts colleges, including the U.S. Military Academy at West Point, is 7:1. See Jordan Friedman, “Twenty-One Liberal Arts Colleges with Lowest Student-Faculty Ratios,” *U.S. News and World Report*, April 19, 2016, available at <www.usnews.com/education/best-colleges/the-short-list-college/articles/2016-04-19/21-liberal-arts-colleges-with-the-lowest-student-faculty-ratios>.

²⁹ Scales, “Too Busy to Learn.”

³⁰ Yeager, *Provost Concept for Learning and Technology Center White Paper*.

³¹ An “advisor” may serve as a “mentor,” but the roles are not the same. An advisor oversees student work, monitors progress, and verifies compliance with program requirements. A mentor provides advisory guidance while also serving as an established scholar invested in enhancing the competencies and professional standing of a mentee who is viewed as a scholar in development. See Angela Mays, “The Difference Between ‘Advisors’ and ‘Mentors,’” American Society of Animal Science Web site, August 31, 2011, available at <www.asas.org/taking-stock/blog-post/taking-stock/2011/08/31/the-differences-between-advisors-and-mentors>; and Tina M. Harris and Celeste N. Lee, “Wicked Problems Forum: Mentoring in Higher Education,” *Communication Education* 68, no. 1 (January 2019), 103–113.

³² See Larry D. Miller and Laura A. Wackwitz, “Writing, Integrity, and National Security,” *Joint Force Quarterly* 79 (4th Quarter 2015), 57–62.

³³ Richard H. Kohn, “Letter to the Editor,” *Joint Force Quarterly* 74 (3rd Quarter 2014), 2.

³⁴ U.S. Constitution, preamble, available at <www.usconstitution.net/xconst_preamble.html>.

³⁵ See Harlan K. Ullman, *A Handful of Bullets: How the Murder of Archduke Franz Ferdinand Still Menaces the Peace* (Annapolis, MD: Naval Institute Press, 2014), 11–30.

³⁶ Martin E. Dempsey, “Investing in the Minds of Future Leaders,” *Joint Force Quarterly* 74 (3rd Quarter 2014), 4–5.

³⁷ Ricks, *The Generals*, 458, notes that American military culture “take[s] a dim view of writing for professional journals.” The elective titled Writing for Publication is no longer offered at the U.S. Army War College (USAWC), and *The Army War College Review*, a refereed online journal of award-winning student research and writing, was recently deleted from the USAWC Press product line.



Paul Sobol, survivor of Auschwitz Concentration Camp, watches presentation about horrors of Holocaust during special Holocaust Remembrance Day observance, April 12, 2019, at Supreme Headquarters Allied Powers Europe, Belgium (U.S. Army/Pierre-Etienne Courtejoie)

Expanding Atrocity Prevention Education for Rising U.S. National Security Leaders

By David Wigmore

Sixty-six years since the Holocaust and 17 years after Rwanda, the United States still lacks a comprehensive policy framework and a corresponding interagency mechanism for preventing and responding to mass atrocities and genocide. This has left us ill prepared to engage early, proactively, and decisively to prevent threats from evolving into large-scale civilian atrocities.

—SCOTT STRAUS, *FUNDAMENTALS OF GENOCIDE AND MASS ATROCITY PREVENTION*

David Wigmore is a Visiting Faculty Member at the National Counterterrorism Center and an Instructor in the War and Conflict Studies Department, College of International Security Affairs, at the National Defense University.

D eployed globally, U.S. diplomatic, intelligence, and military personnel are positioned to identify and report potential warning signs of atroci-

ties by foreign actors, in some cases beyond the capabilities and reach of the media or private organizations. Some U.S. Government-sponsored education



Young girl participates in United Nations Headquarters 16th commemoration of International Day of Reflection on 1994 Genocide in Rwanda, honoring victims of genocide with flowers, United Nations, New York, April 7, 2010 (Courtesy United Nations/Paulo Filgueiras)

in atrocity awareness and prevention exists for military and civilian professionals; however, this education is not offered to a key set of rising leaders and does not focus enough on prevention before the onset of violence. This gap could be covered by a new course at the senior Service college (SSC) level. The practical objective is to equip rising military and civilian national security leaders in 10-month SSC master's programs to recognize and report on potential atrocity warning signs in addition to regular duties. The reporting mechanism that a course prescribes would activate when other reporting mechanisms are lacking or when no similar information has been reported.

Upstream Prevention

U.S. Government education on atrocities has evolved from awareness to intervention, the latter in keeping with the aforementioned military training, but can do more to teach skills that lead to

actions to prevent them. It also can do more to foster prevention regardless of whether there are, will be, or might be U.S. military operations. This is known as "upstream prevention."

One type of U.S. Government school convenes rising interagency national security professionals for nearly a year to study issues of strategic significance. In their 10-month programs, SSCs educate students mostly at the rising O-5 to O-6 (military), FS-2 to FS-1 (foreign service), and GS-14 to GS-15 (civil service) levels. This is a critical juncture where officials who have demonstrated the potential to exercise good judgment on issues of national significance will, after graduation, move into senior management positions and assume roles with increasingly strategic influence. Students take core courses; they also take electives based on their specializations and interests. The proposed course is intended as a core course, but there is some room for flexibility, which is discussed later.

From Understanding to Action

Outreach by the author revealed that courses of various lengths and with varying amounts of content on atrocity history and context exist at U.S. Service academies, the U.S. Agency for International Development (USAID), the Army Command and General Staff College, some single-Service SSCs, and the Department of State. Most teach awareness through studying past atrocities and genocide (such as the Holocaust) and may include local museum visits, but if they address prevention actions directly, they do so largely in an operational context of a U.S. military or developmental agency intervention, often after the onset of violence, to prevent further violence. This is noble and laudable but may be too late to prevent some atrocities. In contrast to upstream prevention, prevention in the context of military or development operations is referred to as "proximate prevention."

At the Joint Professional Military Education (JPME) II level, including at the National Defense University (NDU) in Washington, DC—the flagship U.S. institution for joint Service and interagency national security education—no course exists that emphasizes how to recognize and assess the often nonviolent warning signs of atrocities. The goal is to warn senior U.S. decisionmakers who can leverage all elements of national power, including but not limited to the military, to prevent potential atrocities in the making. The mere threat of U.S. lethality, delivered to the right mala fide actors, could lead to such prevention.

NDU's deliberately ecumenical allotment of places for interagency and multi-Service students and location in the Nation's capital make it an ideal candidate to pilot a new course. Having the Central Intelligence Agency; other Intelligence Community components; the Departments of Energy, Justice, and State; USAID; and other organizations supplying students and in many cases faculty chairs and instructors strengthens the justification for this education to be delivered at NDU.

Humanitarian and Strategic Imperatives

There are humanitarian and strategic imperatives to devote the curricular bandwidth to educate rising leaders at SSCs in atrocity prevention. The type of rising leader who attends an SSC, particularly at the JPME II level, will be tasked with keeping focus increasingly on strategic outcomes.

Rising leaders in the process of gaining a credential necessary to earn general officer/flag officer status as well as their civilian counterparts just below senior level (the senior executive service, senior foreign service, senior intelligence service for CIA staff, and senior national intelligence service for Office of the Director of National Intelligence) staff are in positions of increasing influence in the formulation and execution of policy and strategy.

Key Definitions

For the purposes of this article, the term *mass atrocities* reflects the Army defini-

tion of “widespread and often systematic acts of violence against civilians or other noncombatants including killing; causing serious bodily or mental harm; or deliberately inflicting conditions of life that cause serious bodily or mental harm.”¹ A course should not prescribe a numerical starting point for when something is an atrocity or a mass atrocity. For example, the killing of an entire village of 50 people, or all its adults, or all its men and boys, versus the killing of 8,000 men and boys in Srebrenica can both be considered atrocities. However, for illustrative purposes, the massacre of 8,000 in Srebrenica is considered a *mass atrocity* that was part of the larger Bosnian genocide.²

The term *national security professionals* reflects the interagency civilian and multi-Service military students who attend SSCs. The proposed course objectives and topics of instruction follow.

Proposed Course Objectives and Topics of Instruction

Near-Term Desired Learning

Outcome (1–3 Years). Students should comprehend and be able to apply the thresholds for issuing a report of assessed warning signs, as well as produce a warning report incorporating course-prescribed elements. Students also should remember U.S. legal, policy, and other justifications for engaging in atrocity prevention.

Mid- to Longer Term Desired Learning Outcome (4–5 years). The application of precursor recognition and reporting skills has become second nature and is a trait of more and more ethical U.S. national security leaders. An annually refreshed active minority of rising senior leaders in the military and elsewhere is now prepared to report on assessed atrocity precursors in addition to regular duties, and where no other reporting exists.

Overall Desired Learning Objectives

Although there is no single causal roadmap of acts that lead to atrocities, students should evaluate, analyze, comprehend, and remember stages of atrocities through review of two or three rubrics. Students should know the types

of national responses to atrocity warning signs or actual atrocities.

Scope of Applied Learning. To contribute to preventing atrocities whether they are directly tied to military conflict or not.

Recommended Course Textbooks.

These include Scott Straus's *Fundamentals of Genocide and Mass Atrocity Prevention*³ and Samantha Power's *A Problem from Hell: America and the Age of Genocide*.⁴ Additional mandatory course reading is Alison Des Forges's "Ten Lessons to Prevent Genocide."⁵

Topics of Instruction.

- Why Teach a Specific Set of Atrocity Prevention Skills at SSCs?
- What Is “Active Bystandership”?
- Atrocities and Terrorism
- From Human Security to Responsibility to Protect to Obligation to Prevent: The Evolving Nature of Atrocity Prevention
- Environments Where Atrocities Can Happen and the Phenomenon of “Heroic Prevention”
- Learning to Recognize the Stages of Atrocities

Case Studies.

- Srebrenica
- Misuse of Personally Identifiable Information by Nazi Regime as a Precursor to Mass Deportations and Killings
- Potential U.S. Holocaust Memorial Museum visit with specific learning objectives and follow-up discussion
- Reporting Thresholds, Guidelines, and Requirements
- What to Expect Based on Sending a Report

Justification for a New Course

There are many justifications for teaching atrocity prevention at SSCs. First, if not prevented, killings of targeted unarmed civilian populations will continue to claim many lives. USAID reports that “tens of millions of civilians have lost their lives in the last century in episodes of mass killings.”⁶

A U.S. Military Academy *Pointer View* magazine article posits that “genocide and mass atrocity have killed three to four times as many people as war.”⁷ As not all warning signs are violent or sensational, educating national security practitioners to recognize potential precursors is critical. Events that fall below a media reporting threshold may nevertheless warrant being shared with policymakers.

Second, the cost of prevention likely is less than the cost in lives and national treasure of response. National security practitioners, including military leaders, have an ethical obligation to safeguard both. Relatedly, U.S. national security professionals have a moral and ethical obligation to promote human rights, justice, safety, and security.⁸ Accordingly, the proposed atrocity prevention education aligns with the JPME call for character development—specifically, ethical and moral leadership.⁹

Third, on January 24, 2019, the Elie Wiesel Genocide and Atrocities Prevention Act of 2018 was signed into law. The law, which requires U.S. Government-wide efforts to increase early warning capacities,¹⁰ received broad bipartisan support and could be leveraged to generate funding for a new course.¹¹

Fourth, if atrocity prevention continues to be viewed exclusively through a military-operational lens, the full potential of U.S. talent and technology may not be leveraged for prevention, especially upstream prevention. It is also important to point out that there is no guarantee that every atrocity can be prevented, but the United States has an opportunity to increase its capacity with a new course.

Fifth, for some intelligence analysts, the traditional focus may be on strategic decisionmaking in capital cities but not events that affect populations in the countryside. This can create scenarios where atrocity precursors could go unreported or atrocities may occur.

Sixth, in an era of renewed Great Power competition, there is a risk to U.S. credibility in doing nothing in the face of atrocity warning signs. This is discussed later in detail.

Seventh, atrocities occur in the context of armed conflicts more often than not.¹² According to the U.S.-based nonprofit Stanley Foundation, “Since 1945, two-thirds of episodes of mass killing—defined in the study as a minimum of 5,000 civilians killed intentionally—occurred within the context of an armed conflict. Between 1980 and 2010, that figure was 85 percent.”¹³ Conflicts that may not represent existential threats to U.S., ally, or partner interests nevertheless may be breeding grounds for atrocities. Doing nothing could harm U.S. credibility.

Eighth, Executive Order 13279, dated May 18, 2016, states that the “Department of Defense (DOD) shall continue to develop joint doctrine and training that support mass atrocity prevention and response operations and shall address mass atrocity prevention and response as part of its general planning guidance to combatant commands and [S]ervices.”¹⁴

Ninth, early recognition of potential atrocity warning signs enhances a proactive posture for fulfilling the international moral obligation to prevent atrocities in the spirit of the United Nations (UN) policy of Responsibility to Protect (R2P). Pillar 3 of R2P asserts, “If a state is manifestly failing to protect its populations, the international community must be prepared to take appropriate collective action, in a timely and decisive manner and in accordance with the UN Charter.”¹⁵ Academic discussion on the efficacy of Pillar 3 centers on its dependence on a UN Security Council whose permanent members have differing strategic interests and where competing Great Powers have played the role of spoiler. A new course’s prescribed warnings do not depend on whether R2P is approved for a given situation; instead, a course would seek to empower action at the individual practitioner level—in the spirit of, but not tethered to, Pillar 3—akin to “see something, say something.”

Finally, in a 2016 report titled *An Assessment of USG Atrocity Prevention Training Programs*, a former advisor on atrocity prevention to the Secretary of Defense reiterated the 2011 Presidential

Study Directive on Mass Atrocities recommendation that DOD “mandate and fund the National Defense University to develop a semester-long course on atrocity prevention.”¹⁶ The 2016 report also noted the following:

*Few USG-run educational institutions offer the kinds of courses that impart more advanced atrocity prevention concepts. Currently, the Department of State Foreign Service Institute, the USAID University, and NDU do not offer in-depth courses on atrocity prevention. Exceptions are found in the DOD universe: the three [S]ervice academies, the Army Command and General Staff College, and the Army War College regularly offer at least one semester-long course on the Holocaust, and/or genocide studies. In almost all of these cases, however, the courses are the result of the individual initiative of professors and instructors with personal or professional interest in the topic. Therefore, it is not clear whether the electives would survive their departure or retirement. Only West Point, with its Center for Holocaust and Genocide Studies, has created a permanent infrastructure—and even in that case, it resulted from the support of private donors rather than a formal institutional mandate. A related issue is a lack of scaffolding that could help ensure that those who take training at different points in their career are learning concepts comparable to their experience and needs. The lack of any mandatory training contributes to the problem.*¹⁷

Military and Civilian Scholarship and Literature

A 2012 NDU thesis by a Coast Guard officer spoke of the imperative for U.S. policy to include diplomatic and military measures to prevent atrocities. He also pointed out that some geographic combatant commands cover more countries vulnerable to atrocities than others.¹⁸ In a 2014 monograph, an Army Command and General Staff College student wrote that “the military is not properly trained at the individual level” for atrocity prevention operations. The author framed and justified



Memorial with 17,000 quarry stones marks site of Nazi Germany's extermination camp called Treblinka II, in occupied Poland, where approximately 870,000 to 925,000 Jews and others were murdered, November 6, 2010 (Courtesy Adrian Grycuk)

atrocity prevention along a Clausewitzian model, arguing that both war and genocide are extensions of politics.¹⁹

Additional publications stand out in informing a course syllabus. The specialized and expertly crafted Mass Atrocity Response Operations (MARO) and Mass Atrocity Prevention and Response Operations (MAPRO) manuals²⁰ fall under U.S. peace and stabilization operations; prevention in this context is the aforementioned proximate prevention.²¹ While valuable for some practitioners to learn, the gap the proposed course seeks to address is the teaching of equally and universally relevant upstream-prevention skills.²² MARO and MAPRO will be

discussed, but should not be the backbone of a new course.

Moreover, in "*A Problem from Hell*: *America and the Age of Genocide*", mentioned above, former UN Ambassador Samantha Power notes that "in the arena of foreign policy, morality is like the emperor's clothes: everyone pretends it is there. Despite lofty rhetoric by politicians of all colors, in the end Realpolitik overwhelms Moralpolitik."²³ Nevertheless, Great Power competition, as reflected in the 2018 National Defense Strategy,²⁴ may do well to be informed by *Moralpolitik*, where the U.S. comparative advantage in morality is leveraged to help the United States

and partners prevail against morally ambivalent competitors.

Atrocity Prevention and Great Power Competition

China's People's Liberation Army publications argue that China will take on a greater humanitarian intervention role and that they view such operations as a way to project soft power, gain experience, and expand their global footprint and reach.²⁵ Accordingly, Beijing's basing strategy could be sold as creating logistical hubs to assist humanitarian operations, including in support of its Belt and Road Initiative.²⁶ The U.S. intention to leverage its perceived moral obligation



Wall of names at Srebrenica–Potočari Memorial and Cemetery for the Victims of 1995 Genocide, near Srebrenica, March 18, 2009 (Courtesy Michael Büker)

to engage globally grates on the Chinese military and is referred to as “the American attitude that ‘I am responsible for every place under the sun.’”²⁷

For the moment, China’s efforts to project soft power through humanitarian assistance appear confined to noncombatant evacuation operations, famine aid, and disaster relief, mimicking what it has seen the United States do. Its forays into humanitarian work are increasing, however.²⁸ Reduction of global crises could make it more difficult for China to justify military expansion on “humanitarian” grounds.²⁹ This informs and further justifies an SSC mass atrocity prevention syllabus by suggesting that there are strategic benefits to the United States expanding its mass atrocity prevention capacity, which would be improved by educating more officials.³⁰

This article assesses that only the United States can lead in atrocity prevention based on its moral underpinnings, strong tradition of equipping national security professionals with ethics, and the reach and might of the Nation itself.

There will be strategic challenges and even dilemmas. For example, the treatment of Uyghurs in Xinjiang Province provides an example of how China manipulates moral outrage. A cycle of *escalating to deescalate*, where each “new normal” is worse for a vulnerable population than the status quo ante, may be in store. Furthermore, China’s manipulation of humanitarian issues for its own gain has played out with Beijing’s votes on quashing UN reporting on the plight of Rohingya Muslims.³¹

David Shambaugh suggests that China’s strategic culture is one of

parabellum, or “beside war.”³² U.S. military might deters China, but China competes with the United States on other fronts, leveraging its perceived or actual comparative advantages. Shambaugh implies that either the United States address this or risk strategic diminishment, perhaps without a shot being fired. Not every atrocity may be prevented, but increased U.S. focus on atrocity prevention could keep its “moral suasion” reservoir filled in a period of Great Power competition where attracting partners based on shared interests—including beyond the purely economic—remains a U.S. comparative advantage.³³

Further Considerations and Recommendations

A proposed course is not intended to equip SSC students to meet a prosecu-

torial threshold of proof that an atrocity could occur or is occurring, but rather to be able to provide early warning to higher level decisionmakers that conditions may be favorable for one to occur.

A syllabus must incorporate a validated formula where circumstances cross a threshold requiring communication. Although atrocity environments can be complex, a notional diagnostic framework and reporting threshold will be designed for busy professionals whose sole occupation is not atrocity precursor diagnosis.

Making reporting of assessed potential atrocity precursors a critical intelligence requirement for combatant commanders and issuing a similar directive for Intelligence Community personnel would strengthen the impact of the new learning. Having military critical intelligence requirements and Intelligence Community directives overlap is preferable to having gaps between them, but care should be taken to ensure they do not contradict one another. A new course also may require new instructions in the Foreign Affairs Manual.

It merits mentioning that while this article is not about atrocious acts that could be committed by unethical U.S. personnel, it might raise consciousness. Related to ethics, a study conducted among civilian and military students at NDU indicates that SSC-educated civilians are more likely to engage in ethical behavior, even if it is not specifically required, based on the ends justifying the means in a scenario—perhaps suggesting that civilian national security professionals might be more inclined than their military officer counterparts to issue some kind of report of observed atrocity precursors regardless of reporting requirements. In contrast, following existing guidance and maintaining norms were the higher motivation to engage in ethical behavior for military SSC students who were part of the study.³⁴ Regardless of the prevailing pathways to engaging in ethical behavior that the study results indicate, learning atrocity prevention skills would be useful for civilian and military SSC students alike, as well as being in the U.S. interest.

Inauguration of a new course would benefit from one or more statements from the Chairman of the Joint Chiefs of Staff and other leaders whose personnel attend SSCs that reporting on assessed atrocity warning signs is authorized, expected, and required. SSC provosts/vice presidents of academic affairs and the head of Joint Force Development (J7) also must endorse a proposal. Whether the reporting requirement is or should be the purview only of officials who are recipients of the prescribed education should be a decision for individual departments and agencies to make; however, an effort should be made to cultivate an interagency professional culture that is geared toward preventing atrocities. The more places such education is provided, the more this will be the case.

The proposed syllabus, albeit truncated above for the purposes of this article, is intended to fit a semester-long, mandatory core course for all SSC military and civilian students in 10-month programs. A semester-long elective may be a second-best scenario if the curricular bandwidth will not allow for all to take such a course. A hybrid may be an elective for some and a mandatory course depending on a student's chosen program. A third, less desirable option (because it may leave out important topics) would be to teach precursor recognition and reporting thresholds as a shorter module. Teaching key elements as part of distance learning or a mobile course also should be explored.

Periodically, based on classroom observations and student surveys, a syllabus should be evaluated and modified as warranted. Readings should be reviewed annually for potential updates. Educators should consider incorporating an updated version of the Shrouded Horizons tabletop exercise from NDU's Center for Applied Strategic Learning into a syllabus.³⁵ A course could fall under ethics or leadership departments or be cross-coded.

Faculty retention and turnover will contribute to a course's endurance and vitality. Atrocity prevention education will benefit from individual and institutional

champions. Institutions such as the U.S. Holocaust Memorial Museum can serve as resources and reservoirs of support. Continued engagement with the museum is recommended.

As a near-term next step, the small but diverse group of interested parties and experts who have already met to discuss a new course should host a symposium that calls on additional experts and additional representatives from NDU.

Conclusion

Atrocities happen in the proverbial shadows or in plain sight, in slow motion or fast, noisily or quietly, but not without warning signs.³⁶ Not all are overtly violent. This article covers the strategic and humanitarian benefit, surrounding literature, relative cost savings, and additional justifications for increasing U.S. capacity to recognize and assess potential atrocity warning signs and prevent targeted killings of unarmed civilian populations on and off the battlefield. Accordingly, the article proposes education not limited to any military operational phase. The education applies to the military students prevalent at SSCs and their civilian counterparts who may be slightly lesser in number but are nevertheless well represented in the NDU classroom. The proposed education imparts portable skills relevant to practitioners at home and abroad.

Even if SSCs only taught military students, the proposed education would garner benefits. Continued and increased engagement in atrocity prevention, bolstered by capacity-growing education, would make deposits into a strategic credibility account the United States can draw on later. Including international students in the education may extend the benefit. If the education prevents harm to a single population, it will be worth the effort.

Selection to attend SSCs reflects individual maturity and potential; equipping SSC students with measures to warn about observed atrocity precursors represents a sound investment in the right people. Filling this gap in atrocity prevention education at SSCs will foster a

continuum of educated national security leaders as well as a shared vocabulary and diagnostic toolkit. A new course will educate leaders who may not have had atrocity prevention education previously, and it may even serve to bolster JPME.

For strategic and humanitarian reasons, rising national security leaders should adopt atrocity prevention as a calling and a duty. SSCs, starting with NDU, would do well to fill a gap and devote the curricular bandwidth to equip them to do so. JFQ

Notes

¹ Brian L. Braithwaite, “Mass Atrocities Prevention: The Role and Performance of the United States Army” (Master’s thesis, U.S. Army Command and General Staff College, 2015).

² Susana SáCouto, “Reflections on the Judgment of the International Court of Justice in Bosnia’s Genocide Case against Serbia and Montenegro,” *Human Rights Brief* 15, no. 1 (2007), 1.

³ Scott Straus, *Fundamentals of Genocide and Mass Atrocity Prevention* (Washington, DC: United States Holocaust Memorial Museum, 2016).

⁴ Samantha Power, “*A Problem from Hell*: America and the Age of Genocide (New York: Basic Books, 2013).

⁵ Alison Des Forges, “Ten Lessons to Prevent Genocide,” available at <www.peace.ca/ten_lessons_to_prevent_genocide_.htm>.

⁶ Benjamin A. Valentino, *Final Solutions: Mass Killing and Genocide in the 20th Century* (Ithaca, NY: Cornell University Press, 2004), 1.

⁷ Michelle Eberhart, “Studying Atrocities and Methods of Prevention,” *Pointer View*, October 13, 2016.

⁸ Michael J. Smith, “Humanitarian Intervention: An Overview of the Ethical Issues,” *Ethics & International Affairs* 12 (1998), 63–79.

⁹ Charles Davis and Frederick R. Kienle, “Toward a More Lethal, Flexible, and Resilient Joint Force: Rediscovering the Purpose of JPME II,” *Joint Force Quarterly* 92 (1st Quarter 2019), available at <<https://inss.ndu.edu/Media/News/Article/1760968/toward-a-more-lethal-flexible-and-resilient-joint-force-rediscovering-the-purpo/>>.

¹⁰ “The Elie Wiesel Genocide and Atrocities Prevention Act Becomes Law,” *Invisible Children*, available at <<https://invisiblechildren.com/blog/2019/01/18/elie-wiesel-genocide-and-atrocities-prevention-act-becomes-law/>>.

¹¹ Ibid.

¹² Martin Shaw, *War and Genocide: Organised Killing in Modern Society* (Cambridge, UK: Polity Press, 2003), 43–45.

¹³ Alex J. Bellamy, *Mass Atrocities and Armed Conflict: Links, Distinctions, and Implications for the Responsibility to Prevent*, Policy Analysis Brief (Muscatine, IA: The Stanley Foundation, 2011), 2, available at <<https://stanleycenter.org/publications/pab/BellamyPAB22011.pdf>>.

¹⁴ Executive Order 13729, “A Comprehensive Approach to Atrocity Prevention and Response,” dated May 18, 2016, *Federal Register* 81, no. 99 (May 23, 2016), available at <www.govinfo.gov/content/pkg/FR-2016-05-23/pdf/2016-12307.pdf>.

¹⁵ “About R2P,” Global Centre for the Responsibility to Protect, available at <www.globalr2p.org/about_r2p>.

¹⁶ Charles J. Brown, “An Assessment of USG Atrocity Prevention Training Programs,” U.S. Holocaust Memorial Museum Preventing Genocide, July 18, 2014, available at <[www.ushmm.org/m/pdfs/03282016-USG-Atrocity-Prevention-Training-Assessment.pdf](https://ushmm.org/m/pdfs/03282016-USG-Atrocity-Prevention-Training-Assessment.pdf)>. (Note: Author Charles J. Brown served as Senior Advisor for Atrocity Prevention and Response in the Department of Defense.)

¹⁷ Ibid.

¹⁸ M.S. Furlong, “Preventing Genocide: A Framework for Military Planners” (Master’s thesis, Joint Advanced Warfighting School, 2012).

¹⁹ Anthony L. Volino, “Leveraging the Trinity: A Clausewitzian Framework for Genocide Prevention” (Master’s thesis, U.S. Army Command and General Staff College, School of Advanced Military Studies, 2014).

²⁰ Dwight Raymond et al., *Mass Atrocity Prevention & Response Options: A Policy Planning Handbook* (Carlisle Barracks, PA: U.S. Army Peacekeeping and Stability Operations Institute, 2012).

²¹ Scott Straus, “What Is Being Prevented? Genocide, Mass Atrocity, and Conceptual Ambiguity in the Anti-Atrocity Movement,” in *Reconstructing Atrocity Prevention*, ed. Sheri P. Rosenberg, Tibi Galis, and Alex Zucker (New York: Cambridge University Press, 2016), 17–30.

²² Eli Stamnes, “Speaking R2P and the Prevention of Mass Atrocities,” *Global Responsibility to Protect* 1, no. 1 (February 2009), 70.

²³ Power, “*A Problem from Hell*.”

²⁴ Aaron Mehta, “National Defense Strategy Released with Clear Priority: Stay Ahead of Russia and China,” *Defense News*, January 19, 2018, available at <www.defensenews.com/breaking-news/2018/01/19/national-defense-strategy-released-with-clear-priority-stay-ahead-of-russia-and-china/>.

²⁵ Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China’s Master Plan to Destroy America* (Beijing: PLA Literature and Art Publishing House, 1999).

²⁶ Tania M. Chacho, *Lending a Helping Hand: People’s Liberation Army and Humanitarian Assistance/Disaster Relief* (Colorado Springs: Institute for National Security Studies, 2009).

²⁷ Qiao and Wang, *Unrestricted Warfare*.

²⁸ Andrea Binder and Björn Conrad, *China’s Potential Role in Humanitarian Assistance*, Humanitarian Policy Papers 2 (Berlin: Global Public Policy Institute, 2009).

²⁹ Katri Pynnöniemi and Sinikukka Saari, “Hybrid Influence—Lessons from Finland,” *NATO Review*, June 28, 2017, available at <www.nato.int/docu/review/2017/also-in-2017/lessons-from-finland-influence-russia-policy-security/en/index.htm>.

³⁰ Patrick Porter, “Advice for a Dark Age: Managing Great Power Competition,” *The Washington Quarterly* 42, no. 1 (2019), 7–25.

³¹ Michelle Nichols, “China Fails to Stop U.N. Security Council Myanmar Briefing,” Reuters, October 24, 2018, available at <[www.uk.reuters.com/article/uk-myanmar-rohingya-un/china-fails-to-stop-u-n-security-council-myanmar-briefing-idUKKCN1MY2R8](https://uk.reuters.com/article/uk-myanmar-rohingya-un/china-fails-to-stop-u-n-security-council-myanmar-briefing-idUKKCN1MY2R8)>.

³² David Shambaugh, “China’s Military Views the World: Ambivalent Security,” *International Security* 24, no. 3 (Winter 1999/2000), 52–79, available at <www.belfercenter.org/sites/default/files/files/publication/shambaugh_david_v24n3.pdf>.

³³ Ibid.

³⁴ Raj Agrawal, Kenneth Williams, and B.J. Miller, “An Assessment of Student Moral Development at the National Defense University: Implications for Ethics Education and Moral Development for Senior Government and Military Leaders,” draft, 2019.

³⁵ “Simulation Exercise Examines Atrocity Prevention Board’s Role in Preventing and Responding to Mass Atrocities,” *Human Rights First*, August 17, 2012, available at <www.humanrightsfirst.org/press-release/simulation-exercise-examines-atrocity-prevention-board%E2%80%99s-role-preventing-and->.

³⁶ Nicholas Kristof, “I Saw a Genocide in Slow Motion,” *New York Times*, March 2, 2018, available at <www.nytimes.com/2018/03/02/opinion/i-saw-a-genocide-in-slow-motion.html>.



U.S. and Gulf Cooperation Council forces conduct final field-training event of exercise Eagle Resolve 2017, which focuses on regional challenges associated with asymmetric/unconventional warfare, in Kuwait's Shuwaikh Port, April 6, 2017 (U.S. Army/Frank O'Brien)

The Missing Element in Crafting National Strategy

A Theory of Success

By Frank G. Hoffman

By the end of the 19th century, the study of strategy had become routine for practitioners, but of little interest for theorists. By the end of the 20th century, it had become a matter of endless fascination for theorists, but a puzzle for practitioners.

—LAWRENCE FREEDMAN, “THE MEANING OF STRATEGY, PART II”

Dr. Frank G. Hoffman is a Distinguished Research Fellow in the Center for Strategic Studies, Institute for National Strategic Studies, at the National Defense University.

There are fervent debates today about strategy, especially U.S. grand or national-level strategy.¹ The study of grand strategy is a con-

ceptual minefield.² Gallons of ink have been spent on definitions, but these debates have done little to enhance U.S. strategic thinking or performance.



UH-1Y Venom helicopter takes off from flight deck of USS Boxer, Strait of Hormuz, July 18, 2019 (U.S. Marine Corps/Dalton Swanbeck)

Some academics dismiss national strategies as vain and hubristic, more grandiose than practical plans to obtain goals. Others criticize the tendency in U.S. policy circles to confuse grandiose objects and rhapsodic prose with pragmatic plans and appropriate means. But others contend that policymakers and their military advisors cannot escape the need to intelligently craft strategies to advance the Nation's interests. As Hal Brands notes, "grand strategy is neither a chimera nor an elusive holy grail, but rather an immensely demanding task that talented policymakers have still managed to do quite well."³

Yet scant practical work has been offered to help the next generation of practitioners create strategies in the midst of a disruptive strategic environment. Many books have been written, and numerous laments about lapses in U.S. strategy have been published. There is more art than science to designing a grand strategy, but the practice of strategy has always been a pragmatic art.⁴ Scholars at professional military education (PME) schools admit that more needs to be done to educate the joint community

about the basic process and central, causal logic inherent to sound strategy.⁵ Most schools teach a general and linear process model, and there is a growing recognition about the need for an explicit causal logic in strategy formulation. As noted briefly in this journal 2 years ago, a theory of victory or success should be central to national planning processes.⁶ This is an overlooked element of strategy today both in the classroom and in the U.S. Government. Filling that gap will materially enhance our odds of gaining strategic success in the future and solve the puzzle for strategic practitioners.⁷ It is not a panacea to strategic competence, which involves many elements, but it *is* central to strategic success.

This article examines the theoretical debates over strategy, its constituent elements (ends, ways, and means), and how we have conducted or designed such strategies in the past. Next, it reviews how U.S. national strategies have been constructed in the past, too often overlooking the causal logic that should be the most crucial component of strategic thinking. The article next discusses one technique for formulating an actionable

central idea and another technique for assessing a national strategy and its core elements. Hopefully, this article inspires debate on best practices in strategy formulation and assists those who teach the disciplined process of strategic thinking.

The Silent Ways

Some scholars dismiss the importance of disciplined process and rigorous analysis, contending that strategy "is at the mercy of uncontrollable and often unpredictable political, economic, and military winds and currents."⁸ They stress the need to embrace the study of history and adaptability over foresight in the formulation of grand strategy. Historians find that the informed intuition of great individuals and idiosyncratic process is more important "than a clearly thought through approach to the world."⁹ Others despair of bureaucracy and strategy by committee or formula.¹⁰ Yet process and comprehensive building blocks do have a role in formulating and implementing strategy, grand or otherwise.

In our joint PME community, the construct of strategy as a linkage

among ends/ways/means is a common shorthand recently subjected to acute criticism. It admittedly has the potential to be abused in application.¹¹ It is simplistic and formulaic, if one reduces it to an equation or mindlessly uses it as a recipe. Used in such a way, it would fail to capture the artistry and deep experience required to conceive of national strategy. Yet it captures the basic building blocks and underscores the necessity of tying together the main components of a strategy in a holistic or coherent manner. But the underlying hard work of diagnosis, assumptions, and risk are requisite supporting elements toward crafting a comprehensive approach as well.

The most important and creative aspect of strategy is often silent in the many books on the topic. Critical to the selection of the most appropriate way in a strategy is a hypothesis as to its causal logic. This important concept is rarely discussed in strategic theory. It is largely absent in the writings of today's most prominent thinkers.

As Lawrence Freedman stresses, strategy "is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power."¹² This insight underscores the creative aspect of good strategy: getting more out of a situation than might have been expected by the preponderance of power. Bringing this creative aspect of strategy to the forefront is important, but we need to know more about just how to generate power and how to apply it creatively.

This aspect of strategy is largely absent in U.S. academic literature as well. Western theorists orient on balancing ends and means. Strategy, B.H. Liddell Hart claimed, "depends for success, first and most, on a sound calculation and coordination of the end and the means."¹³ John Lewis Gaddis avoids direct contact with the necessity of causality and defines grand strategy as "the calculated relationship of means to large ends."¹⁴ Later, he found strategy as the alignment of potentially unlimited aspirations with necessarily limited means or capabilities.¹⁵ Other noted scholars emphasize the balancing of ends and means and avoid the

crucial element of ways in their work.¹⁶ One book used in JPME claims that "the marriage of ends and means was the heart of strategy."¹⁷ Another popular book is quiet on the issue of ways as well, stressing the importance of balancing ends and means.¹⁸

This author's own study of the elements of strategy, with an alliterative list of fundamental considerations, also contains a serious similar shortfall. I emphasized the coherence of the three-legged stool but failed to identify causation as a critical factor.¹⁹ As noted by Army War College researchers, however, "Cause-and-effect relationships lie at the heart of all strategic decision-making."²⁰

This consideration is the essence of the strategy function, whereby the strategist exploits the comprehension generated from context and cognitively creates a strategic concept and logic that represent an untested hypothesis that promises to attain policy ends within the means allotted and the constraints that exist. A good strategy must have an internal logic that ties policy to both ways and means to create desired strategic effects. That logic is a continuous thread of thinking that provides strategic intent and informs ways and creates linkages in strategic design that drive the application of means via military operations. This factor is the component that involves calculation, cunning, and the creation of a strategic logic or chain of effects. The strategist's art or most important skill is devising a strategic logic that obtains policy's goals within the given constraints and means.

Military strategists are enjoined to think identifying the center(s) of gravity of the opponent. Grand masters contend that we should ignore this aspect of military theory. They argue that strategists should seek to gain a positional advantage or competitive edge.²¹ One of the keys to sound strategy is focusing power and effort where it will have the greatest impact. The goal is to build and apply situations of strength, positional advantage, or exploiting leverage.

Others have long argued that the targeting of critical vulnerabilities of one's adversary is a better orientation rather

than a source of strength that may well be unassailable.²² Richard Rumelt found that to exploit leverage, a leader has to create and concentrate strengths against a critical vulnerability (not always singular) of the opponent, or what he calls a pivot.²³ This might seem to readers to stand at odds with the Clausewitzian conception of a center of gravity as a source of strength. Rumelt argues that strategy is not only defining sources of strength but also quintessentially about bringing "unexpected strength against discovered weakness. Not simply the deft wielding of power, but the actual discovery of power in a situation, an insight into a decisive asymmetry."²⁴ Other security scholars have made the same point.

Strategy as Hypothesis

This brings us to the central question of how one frames this fundamental determination in the strategy process, especially national strategies. How does a strategy team develop decisive asymmetry and leverage? This is a gap in our understanding of strategy and how to educate students in the formulation of sound strategy. This is the "essence of the strategy function," as stressed in my earlier study, where a strategist "cognitively creates a strategic concept and logic that represents *an untested hypothesis* that promises to attain policy ends within the means allotted and the constraints that exist."²⁵ At the U.S. Army War College, the best academics stress that the establishment of an if/then hypothesis is central to the development of strategy.²⁶ This consideration, "Involves calculation, cunning, and the creation of a strategic logic or chain of effects."²⁷

Overall, strategy formulation should rigorously examine different conceptual approaches framed around a hypothesis about how each strategic option can obtain the specified desired aims. Some military strategies may be thought of as a "theory of victory," obtaining a distinctive goal over an opponent or adversarial coalition. The idea of a theory of victory is well established at the Army War College and studied by students at the Air University.²⁸ But as Eliot Cohen and Jeff



Navy officer answers questions from U.S. and international students of U.S. Army War College during tour of USS America, San Diego, California, March 1, 2017 (U.S. Navy/Kyle Hafer)

Meiser note, it is useful to define strategy, especially grand or national strategies, as a theory of success.²⁹ Given that their purpose is rarely to defeat an adversary but instead is to develop institutional muscle and apply statecraft to desire strategic ends, this is more compelling than victory (and defeat) *per se*.³⁰ The common benefit from both concepts is the requirement to define, in general terms, the causal relationship that converts ways and means into the desired end(s) for testing during strategy refinement.

Meiser goes on to argue that “Defining strategy as a theory of success gives a clear sense of how strategy is distinct from means-based planning and facilitates a superior strategy-making process.” He further notes, “Defining strategy as a theory of success encourages creative thinking while keeping the strategist rooted in the process of causal analysis; it brings assumptions to light

and forces strategists to clarify exactly how they plan to cause the desired end state to occur.”³¹ It is difficult to disagree. This is the critical component of the process and the place where the strategist earns his keep, crafting a solution that describes how proposed efforts gain the achievement of the stated aim. Meiser, however, removes one “sin” of American strategic competency, its *means*-centricity, by overemphasizing the missing aspect of *ways*. But a way-centric application is just as faulty, and also problematic. Ultimately, ways do have to be resourced, either by applying existing sources of power or creating them. In short, Meiser correctly identifies the missing component—a plausible if not rigorous logic embedded in a stated theory of success. There must be more than “stuff happens,” when it comes to ways, and a theory of success has merit because it focuses greater attention to this element

of the process.³² Some find the ends/ways/means framework to be a procrustean tyranny.³³ The only tyranny from the proverbial three-legged stool one escapes from by abandoning such a framework is strategic discipline, founded on a coherent conversion of desired policy ends and means into appropriate action. Instead, we should fix the broken leg with quality strategy education.

Among strategic scholars, Colin Gray seems to have gotten this element of theorizing correct. As he emphasizes in *Teaching Strategy*, “The military planner is, *ipso facto*, a theorist. A plan is a theory specifying how a particular goal might be secured. Until the course of future events unfolds, the chief planner and the commander, who may be one and the same person, are deciding and acting only on the basis of *a theory of success*.³⁴ He goes on to observe that “strategies are theories, which is to say they are



Platoon commander with 2nd Battalion, 8th Marine Regiment, gives professional military education class explaining strategy the Marines of 2/8 used when they landed on Red Beach 3 in November 1943, Betio, Kiribati, July 22, 2018 (U.S. Marine Corps/Timothy Hernandez)

purported explanations of how desired effects can be achieved by selected causes of threat and action applied in a particular sequence.”³⁵ However, despite a wealth of published books on strategic theory and original contributions to strategic thought, Gray offers limited guidance on how to enhance the application of theory to practice.

A rare example of any reference to the inherent theory of success in historical studies is found in *Successful Strategies*. In this book, the editors argue for more than balancing ends and means, as success “hinges almost entirely on the conformity of strategic aims to available military means and *the validity of the theory* according to which the latter are committed.” While failure is often the product of overextension beyond one’s means, this team of editors notes, failure is “perhaps more likely to reflect *mistaken theories of success*.”³⁶ But the editors

never identify who, when, and how political leaders and their strategists define any theory of success in the case studies.

Too often policymakers and military leaders make implicit and untested assumptions about causality. But causality and its underlying hypothesis should be explicit so that it can be rigorously explored for historical and logical validity.

Case Histories

Historical examples may shed some light. President Abraham Lincoln held to a theory of victory and struggled to find a general both to accept and to apply his formulated “way” to preserve the Union.³⁷ George Kennan’s assessment of Russia’s deeply inbred faults was more accurate and logical for exploitation. Thus, the Cold War grand strategy of containment was based on a clear theory of success, predicated on Kennan’s assessment of the ineluctable

internal decay of the Soviet Union.³⁸ The implied theory of success in the Eisenhower-era “New Look” strategy was a not-so-subtle threat to deploy nuclear weapons against challenges large and small. The logic presumed that an emphasis on efficiency through the threat of a massive offensive retaliatory capability would offer a sustainable strategy.³⁹ A reliance on strategic weapons is preferred, Secretary of State John Foster Dulles stated, “Instead of having to try to be ready to meet the enemy’s many choices. That permits . . . a selection of military means instead of a multiplication of means. As a result, it is now possible to get, and share, more basic security at less cost.”⁴⁰ A close reading of the basic document and Dulles’s comments reveals a blurry if not flawed linkage between cause and effects.⁴¹ Moreover, the New Look denied the adversary any real vote. The underlying



John Lewis Gaddis, front left, Robert A. Lovett Professor of Military and Naval History at Yale University, speaks to U.S. Naval War College faculty during Teaching Grand Strategy workshop, in Newport, Rhode Island, August 16, 2012 (U.S. Navy/Eric Dietrich)

logic and its political fallout with allies made it problematic.⁴²

The Nixon administration had a more implicit logic in its national strategy. It understood that U.S. power and credibility had been decremented by the costly and protracted Vietnam War and that domestic support for extended strategic objectives was lacking. Yet the Nixon/Kissinger team remained confident that deft diplomatic maneuvers could buy time, reduce risk, and still sustain U.S. interests.⁴³

The Reagan Presidency also issued a grand strategy, one that reversed the pessimism and constraints of the Eisenhower/Nixon years with a force buildup and the resumption of an ideological element to defeat rather than contain communism.⁴⁴ More specific policy statements on the Soviet Union were issued a year later, with more granularity but little effort at prioritization and no evident logic or theory of success.⁴⁵ Arguably, there was an implicit hypothesis to Reagan's thinking and that of his counselors. It was a successful strategy, credited by many with ending the Cold War.⁴⁶

Arguably, we had a narrow and implicit theory of military victory for Afghanistan in 2002 and in Iraq in 2003, but the United States lacked a more comprehensive theory of success. General David Petraeus's question, "Tell me how this ends?" is poignant.⁴⁷ A theory of success should have answered that question. Such a theory would tie together the desires of policy to what defined ends and ways are being employed. It appears to have been completely lacking.⁴⁸

The first war against Iraq had a limited theory of victory, freeing Kuwait from Saddam's invasion. However, history suggests that it produced a triumph without victory or success over the long run.⁴⁹ The second war against Iraq, after a decade of sanctions and enforcement actions, embraced a larger theory of military victory, yet it too failed to connect to a larger and more politically relevant theory of success.⁵⁰ It is difficult to assess when the United States ever framed a coherent theory of strategic success in Afghanistan that would ensure a politically viable and stable country. The emergent strategy of 2002 effectively and efficiently produced a victory

of retribution against the Taliban and drove it from power. General Stanley McChrystal notably used "strategy of success" several times in his commander's assessment in Afghanistan in the summer of 2009.⁵¹ Yet it remains America's longest war today. Was it predicated on a narrow theory of victory, or did conditions change that required a shift in political aim and an altered strategy?

More recently, a number of new U.S. strategic documents have been issued. The current National Security Strategy has an implicit logic, emphasizing reestablishing a competitive economic basis for prosperity first and a modernized and somewhat larger military to preserve security at home and abroad.⁵² The Pentagon's National Defense Strategy seeks an endstate that restores a favorable balance of power in Asia and Europe. It has an explicit theory of success, predicated around the integration of three major lines of effort: extensive modernization, a strengthened network of allies and partners, and a reformed bureaucracy that drives greater performance and innovation into the joint force.⁵³ The defense innovation enterprise must generate more

value rapidly and at lower costs. Each element of the strategy leverages assumed competencies: joint warfighting, alliance leadership, and an innovation ecosystem. Revitalizing these competencies at scale and in time is the central hypothesis behind the Pentagon's strategy. Both the classified strategy and unclassified summary contain an explicit theory of success.⁵⁴ But it does not appear to have universally reached across the larger joint warfighting community.

Formulating the Theory of Success

How does a policymaker and staff consider constructing a way that solves the central problem or gains the specified desired aim? The question is not "Tell me how this ends?" The central question is "How and why does this work?" Inherent to the strategy is an argument that the solution solves the central aim or problem. This is often derived from a supporting theory. "The role of theory in practicing the art of war," P.J. Maykish argues, "is particularly critical since war provides little or no opportunity for hypothesis testing before life and death is upon the strategist, statesman, warrior, and civilian."⁵⁵ Yet if strategy is applied theory, the merits of the underlying theory (strategic airpower, paralysis, industrial web, "maximum pressure") should be understood and testable.

So how does a national strategy team develop a theory of success? Is a theory of success captured in a single concept like containment, or is it an orchestrated series of strategic activities akin to a campaign plan? This is what Rumelt called a "guiding policy."⁵⁶ Our colleagues in the United Kingdom call this the "big idea," with the Royal Defence College claiming that a "strategy which has no unifying idea is not a strategy. The importance of strategic ideas is often over-looked. The innovative and compelling 'big idea' is often the basis of a new strategy. It must not only bind the ends, ways and means but also inspire others to support it."⁵⁷ This guiding policy or strategic concept may evolve iteratively as the strategy team evaluates different ways and attempts to

Table 1. Causal Mechanisms

Inform/Influence/ Persuade	To disseminate information that shapes perceptions and influences target audiences toward a desired perception.
Negotiate	To bargain with the intent of gaining desired objective(s) while offering to compensate another actor with benefits or compromises.
Induce	To offer incentives, without formal agreement, to influence the actor or an actor in the network of the target actor.
Create	To create an institutional competency or capacity lacking in U.S. institutional capacity or arsenal or one of its allies or partners.
Enable	Security or economic development designed to buttress or augment extant capabilities, to selectively strengthen a desirable component of U.S. or allied state.
Disable	To selectively weaken or make inoperable a critical component of the adversary's defensive system or governance capacity.
Coerce	To threaten to employ direct force or deny the target actor access to a resources or benefit, by threat or sanction, to make the adversary withdraw or settle.
Subdue/Compel	To apply violent force and means to force an adversary to stop doing something already initiated.
Neutralize/ Destroy	To apply violent force in such a way that it severely degrades or eliminates the opponent's capacity to defend itself.

Figure. Notional Strategic Action Mechanisms

- a) Persuade Europeans to extend NATO C2/readiness levels and enable NATO's forward forces in Baltics and Poland to increase deterrence (DOD, DOS, NSC, OMB).
- b) Coerce Russia economically by threatening energy exports with alternative sources and trade barriers, coupled with persuading EU countries to diversify energy imports (DOS, Treasury, Commerce, NSC).
- c) Enable Ukrainian defenders to enhance their training/lethality via advisors and security cooperation programs (DOD/SOCOM, DCSA, DOS, and NSC).
- d) Negotiate with Russia to address its theater missile defense concerns with NATO (DOS, NSC, DOD).

generate advantage by combinations of assets. The strategic cell strives, in the words of the Royal Defence Academy, "to develop the 'big ideas' that could unite ends, ways and means in an innovative and creative manner that confers competitive advantage."⁵⁸

Of course, big ideas are simply that, a generalization. A strategy should convert or amplify that general guiding idea into objectives and actionable tasks to bring it to life. Table 1 presents a number of what might be termed causal mechanisms and their definitions. These are adapted from the National War College's national security strategy primer, which gives considerable attention to approaches in the development of ways.⁵⁹ These range from nonviolent means to total military defeat. Defeat by maneuver and attrition remains viable and necessary causal mechanisms when reduction of the opponent's capacity to resist is needed.⁶⁰

These approaches can be combined in an orchestrated way into the overall strategic approach to develop and justify a causal logic.⁶¹ The National War College employs a technique using "objective instrument packages" to help students operationalize their strategies toward defined objectives.⁶² This is one method of translating a big idea or combination of activities into specific mechanisms across all instruments of national power into a comprehensive strategy of action.

The figure shows a notional suite of such packages that are directed toward a national strategy against Russian aggression in Europe. In support of a strategic concept that seeks enhanced stability and a deterred Russia, this approach exploits combinations of mechanisms that a strategy team must develop.⁶³ The astute team accepts the utility of combinations and sequencing in the formulation of strategy. In developing such a suite or combination

Table 2. Final Assessment Questions

Stages	Critical Considerations
Diagnosis	<p>Does the strategy rigorously diagnose the environment, including friendly and opposing actors?</p> <p>Does the diagnosis account for critical interests and identify where they are at risk?</p> <p>Does the diagnosis identify the central challenge(s) or problem?</p> <p>Does the strategy process reflect the interactive nature of competition and anticipate adversary reactions?</p>
Formulation	<p>Does the strategy generate a better outcome than the initial power position; does it build upon or create new sources of leverage and influence?</p> <p>Does its central logic generate a competitive advantage at the strategic and/or operational level?</p> <p>Does the selected approach have a causal link to desired policy aims?</p> <p>Does the central “way” degrade or defeat the opponent’s strategy or shift the competition to a different domain?</p> <p>Does the strategy and its logic create a compelling argument for consensus and resourcing?</p> <p>Does it apply resources efficiently and gain priority goals within available resources?</p> <p>Does the strategy prioritize objectives and capability investments?</p>
Implementation	<p>Does the strategy acknowledge risks, and prudently address them?</p> <p>Does it have an implementation plan, with metrics or signposts for assessment?</p> <p>Is there a communications plan? Will the strategy be presented to stakeholders/allies?</p>

of approaches, the strategy cell presents an explicit claim for testing and discourse that these activities, properly orchestrated and sequenced, will produce the desired change in context or Russian behavior desired. Collectively, they constitute an implicit theory of success. But that theory should be explicit and debated. Per Professor Tami Davis Biddle’s conception, *if* these actions are taken, *then* the desired political outcome of a deterred Russia and stabilized Ukraine is theoretically feasible.⁶⁴ The strategy team should explore that logic and ensure it is the most feasible course of action and explicitly state it in the strategy.

The multi-instrumental character of national strategies adds complexity to the process and challenges the internal coherence of any strategy. This is the element in the ends/ways/means (plus policy and risks) construct where strategists are most challenged. It may initially come off as formulaic, but it arguably helps ensure some discipline without prescriptively shoehorning the creativity needed by the policy and strategy community.

The figure is entirely illustrative and must be drawn from the diagnosis and strategic assessment conducted earlier in

the strategy’s formulation. That assessment would identify friendly strengths and potentially critical vulnerabilities that could be leveraged. This is why understanding context, founded on a thorough diagnosis, is so critical to strategy. For this reason, the National War College includes a comprehensive understanding of the strategic environment as a fundamental element of the strategic logic process.⁶⁵ The primer also appropriately incorporates risk and cost/benefit analysis as part of its overall strategic logic.⁶⁶

Assessing Strategic Logic

The formulation of a strategy is the first step, and its implementation (including assessment and adaptation) is just as much of the process as the initial diagnosis of the environment. Prior to implementation, a final step is included in most descriptions of the strategy formulation process. The National War College primer includes a set of five evaluative elements, including feasibility, which addresses the ends/ways linkage.⁶⁷ This aspect of the strategy process is a final check on its integrative coherence and logic. A more extended assessment process is offered in table 2. A similar

framework was used during the development of the 2018 U.S. Defense Strategy. Questions 5 through 9 deal with the consideration of ways and causality. The list is not a checklist or a recipe, nor is it a crutch for incurious policymakers or lazy strategists. (Anyone expecting shortcuts and magic potions should shift to another line of work.) Equally, a strategy team that has not thought through the answers to these questions has not completed its mission.

Strategy is more art than science, and the practitioner, whether policymaker or military strategist, needs to recognize the need for humility.⁶⁸ The rigor of the assessment process cannot dilute that reality, but it can mitigate consequences of flawed assumptions, poor decisions, and biases. More important, this set of questions expands on existing doctrine to focus on the causal links in the logic train about its approach, not just the balance of ends to means.

The confluence of contingency and competitiveness produces the need for an additional component—that of constant evaluation of ongoing operations and continuous measurement of progress. “Like a vessel under sail,” notes retired Army strategist Rick Sinnreich, “grand strategy is at the mercy of uncontrollable and often unpredictable political, economic, and military winds and currents, and executing it effectively requires both alertness to those changes and constant tiller correction.”⁶⁹ This is the basis for co-adaptation in form and function as our strategy interacts with the real world and the will of an opponent. We must recognize that in both Great Power competitions and war, the execution of strategy is locked into an iterative relationship, which rests on an inherently dynamic and changing situation and which has to respond to the counters of the enemy.⁷⁰ No strategy should be seen as unalterable or a fixed blueprint written in stone; the critical questions and the central logic should be continuously questioned.⁷¹

Conclusion

Hopefully this brief article catalyzes an extended conversation about causality and theories of success/victory. It

may not clear the messy minefield of grand strategy. If it achieves anything at all, the argument should stimulate the community to turn the corner from debating whether strategy is possible toward exploring what it takes to teach and conduct “good” strategy. Given that U.S. strategies will no longer be privileged with materiel and technological dominance, it behooves the strategic community to refresh its thinking about how to develop creative strategies.

Admittedly, the historical record of grand strategy formulation and execution is littered with failure. Most so-called strategies were not strategies at all.⁷² They were lofty objectives and wish lists of unrelated effort. The role of creative approaches and causation, the central art of strategy, is rarely explored.⁷³ Skeptics of strategy offer few insights on how to improve the development of sound strategy to inform future strategic leaders. This article has attempted to explore the complexity of strategy formulation with an emphasis on the need to improve the ways element of a true and complete strategy. A concept of a *theory of success* for national and grand strategy is proposed as the central idea for such a strategy.

We should not be formulaic in crafting strategy, nor should we dispense with rigorous processes that support causal logic. Devoting more attention to *ways* fills in the black hole, enhances the art of sound strategy, and resolves a key puzzle for practitioners. JFQ

I thank my colleagues at the National War College, my students, and Dr. Jeff Meiser of the University of Portland for stimulating this article. Colonel Dwight Phillips, USA; Colonel Paul J. Maykish, USAF; Mr. Michael Davies; and an anonymous peer reviewer provided insightful comments.

Notes

¹ Richard K. Betts, “The Grandiosity of Grand Strategy,” *The Washington Quarterly* 42, no. 4 (Winter 2020), 7–22.

² Rebecca Friedman Lissner, “What Is Grand Strategy? Sweeping a Conceptual Minefield,” *Texas National Security Review* 2, no. 1 (November 2018), 53–73.

³ For the former, see Simon Reich and Peter Dombrowski, *The End of Grand Strategy: U.S. Maritime Operations in the 21st Century* (Ithaca, NY: Cornell University Press, 2017), 1, 161. For a more optimistic perspective, see Hal Brands, *What Good Is Grand Strategy? Power and Purpose in American Statecraft from Harry S. Truman to George W. Bush* (Ithaca, NY: Cornell University Press, 2014), 190–191.

⁴ Hew Strachan, “Strategy in Theory; Strategy in Practice,” *Journal of Strategic Studies* 42, no. 2 (2019), 188.

⁵ Andrew A. Hill and Stephen J. Gerras, “Stuff Happens: Understanding Causation in Policy and Strategy,” *Parameters* 48, no. 2 (Summer 2018), 13.

⁶ James Hasik, “Beyond the Third Offset: Matching Plans for Innovation to a Theory of Victory,” *Joint Force Quarterly* 91 (4th Quarter 2018), 14–21.

⁷ Linda Robinson et al., *Improving Strategic Competence: Lessons from 13 Years of War* (Santa Monica, CA: RAND, 2017). For a broad overview of strategic thinking and advice on enhancing U.S. national strategy formulation, see Mark Cancian et al., *Formulating National Security Strategy: Past Experience and Future Choices* (Washington, DC: Center for Strategic and International Studies, 2017).

⁸ Richard Hart Sinnreich, “Patterns of Grand Strategy,” in *The Shaping of Grand Strategy: Policy, Diplomacy, and War*, ed. Williamson Murray, Richard Hart Sinnreich, and James Lacey (New York: Cambridge University Press, 2011), 256.

⁹ Williamson Murray, “Thoughts on Grand Strategy,” in Murray, Sinnreich, and Lacey, *The Shaping of Grand Strategy*, 9.

¹⁰ MacGregor Knox, “Conclusion,” in *The Making of Strategy: Rulers, States, and War*, ed. Williamson Murray, MacGregor Knox, and Alvin Bernstein (Cambridge: Cambridge University Press, 1994), 615–621.

¹¹ Jeffrey W. Meiser, “Ends + Ways + Means = (Bad) Strategy,” *Parameters* 46, no. 4 (Winter 2016), 81–91.

¹² Lawrence Freedman, *Strategy: A History* (Oxford: Oxford University Press, 2016), xii.

¹³ B.H. Liddell Hart, *Strategy* (London: Faber & Faber, 1967), 322.

¹⁴ Cited in William C. Martel, *Grand Strategy in Theory and Practice* (New York: Cambridge University Press, 2015), 32.

¹⁵ John Lewis Gaddis, *On Grand Strategy* (New York: Penguin, 2018), 21.

¹⁶ Paul Kennedy, ed., *Grand Strategy in War and Peace* (New Haven: Yale University Press, 1991), 4; Martel, *Grand Strategy in Theory and Practice*, 36, 55–56, 341.

¹⁷ Terry L. Diebel, *Foreign Affairs Strategy: Logic for American Statecraft* (New York: Cambridge University Press, 2007), 181.

¹⁸ Brands, *What Good Is Grand Strategy*, 196, 199.

¹⁹ F.G. Hoffman, “Grand Strategy: The Fundamental Considerations,” *Orbis* 58, no. 4 (Fall 2014), 472–485.

²⁰ Hill and Gerras, “Stuff Happens,” 14.

²¹ Lawrence Freedman, “Stop Looking for the Center of Gravity,” *War on the Rocks*, June 24, 2014, available at <<https://warontherocks.com/2014/06/stop-looking-for-the-center-of-gravity/>>.

²² Joseph Strange and Richard Iron, “Center of Gravity: What Clausewitz Really Meant,” *Joint Force Quarterly* 35 (4th Quarter 2004), 20–27.

²³ Richard P. Rumelt, *Good Strategy/Bad Strategy: The Difference and Why It Matters* (New York: Crown Publishing Group, 2011), 85, 97–98, 101–102. Rumelt contends, “Finding such crucial pivot points and concentrating force on them is the secret of strategic leverage.”

²⁴ Rumelt, cited in Andrew Krepinevich and Barry Watts, *Regaining Strategic Competence* (Washington, DC: Center for Strategic and Budgetary Assessment, 2009), 15; Lukas Milevski, “Asymmetry Is Strategy, Strategy Is Asymmetry,” *Joint Force Quarterly* 74 (4th Quarter 2014), 77–83.

²⁵ Hoffman, “Grand Strategy,” 469. Emphasis in original.

²⁶ Tami Davis Biddle, *Strategy and Grand Strategy: What Students and Practitioners Need to Know* (Carlisle Barracks, PA: U.S. Army War College Press, 2015), 2.

²⁷ Hoffman, “Grand Strategy,” 469.

²⁸ For a general discussion, see J. Boone Bartholomees, “Theory of Victory,” *Parameters* (Summer 2008), 25–36; P.J. Maykish, “Upstream: How Theory Shapes the Selection of Ways in Strategy” (Ph.D. diss., School of Advanced Air and Space Studies, 2016).

²⁹ Eliot A. Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime* (New York: Free Press, 2002), 33, 177, 212.

³⁰ For an example of this, see Hal Brands and Zack Cooper, “After the Responsible Stakeholder, What? Debating America’s China Strategy,” *Texas National Security Review* 2, no. 2 (February 2019), 71.

³¹ Meiser, “Ends + Ways + Means = (Bad) Strategy,” 86.

³² Hill and Gerras, “Stuff Happens,” 13–25.

³³ Matt L. Cavanaugh, “It’s Time to End the Tyranny of Ends, Ways, and Means,” Modern War Institute, July 24, 2017, available at <<https://mwi.usma.edu/time-end-tyranny-ends-ways-means/>>.

³⁴ Colin S. Gray, *Schools for Strategy: Teaching Strategy for 21st Century Conflict* (Carlisle Barracks, PA: Strategic Studies Institute, November 2009), 44. Emphasis added.

³⁵ Colin S. Gray, *Strategy and Defence Planning: Meeting the Challenge of Uncertainty* (Oxford: Oxford University Press, 2014), 30.

³⁶ Williamson Murray and Richard Hart Sinnreich, eds., *Successful Strategies: Triumphing in War and Peace from Antiquity to the Present* (Cambridge: Cambridge University Press, 2014), 439–440. Emphasis added.

³⁷ Kenneth T. Williams, *Lincoln Finds a General: A Military Study of the Civil War*, vol. 3 (New York: Macmillan, 1952); Williamson Murray and Wayne Wei-Siang Hsieh, *A Savage War: A Military History of the Civil War* (Princeton: Princeton University Press, 2016), 167–171, 357–361.

³⁸ On George F. Kennan and containment, see John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War* (Oxford: Oxford University Press, 2005).

³⁹ *A Report to the National Security Council [NSC] by the Executive Secretary on Basic National Security Policy*, NSC Memorandum #162/2 (Washington, DC: The White House, October 30, 1953), 5, available at <<https://fas.org/irp/offdocs/nsc-hst/nsc-162-2.pdf>>.

⁴⁰ Quoted in Bernard Brodie, *Strategy in the Missile Age* (Princeton: Princeton University Press, 1959), 248–249.

⁴¹ Gaddis, *Strategies of Containment*, 125–159.

⁴² Patrick J. Garrity, “A New Look at the New Look,” *Claremont Review of Books*, December 14, 2012, available at <www.claremont.org/crb/basicpage/a-new-look-at-the-new-look/>.

⁴³ Brands, *What Good Is Strategy?* 59–100; Dan Caldwell, “The Legitimation of the Nixon-Kissinger Grand Design and Grand Strategy,” *Diplomatic History* 33, no. 4 (September 2009), 633–652.

⁴⁴ National Security Decision Directive (NSSD) 32, *U.S. National Security Strategy* (Washington, DC: The White House, May 20, 1982).

⁴⁵ NSSD 75, *U.S. Relations with the USSR* (Washington, DC: The White House, January 17, 1983).

⁴⁶ Thomas Mahnken, “The Reagan Administration’s Strategy Toward the Soviet Union,” in Murray and Sinnreich, *Successful Strategies*, 403–431; William Imboden, in *The Power of the Past: History and Statecraft*, ed. Hal Brands and Jeremy Suri (Washington, DC: Brookings Institution Press, 2016), 155–166; Brands, *What Good Is Strategy?* 102–142.

⁴⁷ Linda Robinson, *Tell Me How This Ends: General David Petraeus and the Search for a Way Out of Iraq* (New York: PublicAffairs, 2008).

⁴⁸ Craig Whitlock, “Stranded Without a Strategy,” *Washington Post*, December 9, 2019, A1, A12–A15.

⁴⁹ U.S. News and World Report, *Triumph Without Victory: The Unreported History of the Persian Gulf War* (New York: Crown, 1992).

⁵⁰ Michael J. Mazarr, *Leap of Faith: Hubris, Negligence, and America’s Great Foreign Policy Tragedy* (New York: PublicAffairs, 2019), 387–415.

⁵¹ Matthew C. Brand, *General McChrystal’s Strategic Assessment: Evaluating the Operating Environment in Afghanistan in the Summer of 2009*, Air Force Research Institute Paper 2011-

1 (Maxwell Air Force Base, AL: Air University Press, 2011), available at <https://media.defense.gov/2017/jun/19/2001765050/-1/-1/0/ap_brand_mcchrystals_assessment.pdf>.

⁵² *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017).

⁵³ *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge* (Washington, DC: Department of Defense, January 2018).

⁵⁴ Ibid., 1. The penultimate paragraph states, “A more lethal, resilient, and rapidly innovating Joint Force, combined with a robust constellation of allies and partners, will sustain American influence and ensure favorable balances of power that safeguard the free and open international order.”

⁵⁵ Maykish, “Upstream,” 4.

⁵⁶ Richard Rumelt, “The Perils of Bad Strategy,” *McKinsey Quarterly* (June 2011), available at <www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-perils-of-bad-strategy>.

⁵⁷ The Royal College of Defence Studies, *Getting Strategy Right (Enough)* (London: Ministry of Defence, 2017), 20.

⁵⁸ Ibid., 51.

⁵⁹ Steven Heffington, Adam Oler, and David Tretler, eds., *A National Security Strategy Primer* (Washington, DC: NDU Press, 2019), 37–40, available at <<https://nwc.ndu.edu/Portals/71/Documents/Publications/NWC-NDU-Primer.pdf?ver=2019-07-30-105821-630>>. The list proposed herein adds “Inform” to more distinctly operationalize the informational instrument of national power. This adapted list dropped “Eradicate” but adds “Create.” This was added to support the development of capability or means creation function of national strategies. National strategies may need to create new functions or activities.

⁶⁰ On the tendency to seek short wars, see Cathal J. Nolan, *The Allure of Battle: How Wars Are Won or Lost* (New York: Oxford University Press, 2017).

⁶¹ See Joint Doctrine Note 1-18, *Strategy* (Washington, DC: The Joint Staff, April 25, 2018), III-1-III-3. These are derived from the defeat and stability mechanisms in joint operational art. See Joint Publication 5-0, *Joint Planning* (Washington, DC: The Joint Staff, June 16, 2017), IV-31-IV-33.

⁶² The concept of an “objective instrument package” is drawn from Diebel, *Foreign Affairs Strategy*, 181.

⁶³ The idea of a team rejects the notion of a singular master strategist, as debunked by Lawrence Freedman, “The Master Strategist Is Still a Myth,” *War on the Rocks*, October 14, 2014, available at <<https://warontherocks.com/2014/10/the-master-strategist-is-still-a-myth/>>.

⁶⁴ Biddle, *Strategy and Grand Strategy*.

⁶⁵ Heffington, Oler, and Tretler, *A National Security Strategy Primer*, 7–14. See also Hoffman, “Grand Strategy,” 475–476.

⁶⁶ Ibid., 43–48. Cost/risk analysis as a necessary aspect of a strategist’s tool kit, as noted by Francis J.H. Park, “A Dialogue on Strategy,” *Parameters* 47, no. 1 (Spring 2017), 126–127.

⁶⁷ The National War College uses the phrase *viability assessment*. See Heffington, Oler, and Tretler, *A National Security Strategy Primer*, 45–46.

⁶⁸ Strachan, “Strategy in Theory; Strategy in Practice,” 188.

⁶⁹ Richard H. Sinnreich, in Murray, Sinnreich, and Lacey, *The Shaping of Grand Strategy*, 256.

⁷⁰ Hew Strachan, “Strategy and Contingency,” *International Affairs* 87, no. 6 (November 2011), 1281–1296.

⁷¹ Hal Brands, *The Promise and Pitfalls of Grand Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2012), 49; Hoffman, “Grand Strategy,” 481.

⁷² Freek Vermeulen, “Many Strategies Fail Because They’re Not Actually Strategies,” *Harvard Business Review*, November 8, 2017, available at <<https://hbr.org/2017/11/many-strategies-fail-because-theyre-not-actually-strategies>>.

⁷³ Lukas Milevski, *Grand Strategy Is Attraction: The Logic of Integrating Various Forms of Power in Conflict* (Carlisle Barracks, PA: U.S. Army War College Press, April 2019).



Fire controlman installs radiation cover onto Phalanx close-in weapon system aboard USS *Russell*, January 29, 2020, Pacific Ocean (U.S. Navy/Sean Lynch)

The Joint Force Needs a Global Engagement Cycle

By Gregory M. Tomlin

Both revisionist powers and rogue regimes are competing across all dimensions of power. They have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals.

—2018 NATIONAL DEFENSE STRATEGY

Lieutenant Colonel Gregory M. Tomlin, USA, Ph.D., is Chief of the Targeting Doctrine and Policy Branch, Directorate for Intelligence, Joint Staff J2.

Step into any joint or coalition operations center and you will find planners, intelligence analysts, and operators bustling between working groups and decision boards related to the synchronization of joint

fires. From developing target systems that support the commander's objectives, to validating and prioritizing individual targets, to assigning forces and assessing mission execution, the Joint Targeting Cycle (JTC) often



Lieutenant Commander Erika Schilling, left, and Lieutenant (junior grade) Natalie Spritzer teach Helping Babies Breathe class to local Chuukese women and girls during largest annual multinational humanitarian assistance and disaster relief preparedness mission conducted in Indo-Pacific, Pacific Partnership 2019, in Chuuk, Federated States of Micronesia, March 31, 2019 (U.S. Navy/Tyrell K. Morris)

drives the battle rhythm for combat operations. This process enables a staff to match available capabilities with desired lethal and nonlethal effects against an adversary, and it synchronizes intelligence, surveillance, and reconnaissance (ISR) efforts with the deployment of ground, maritime, air, and cyber assets responsible for executing joint fires.

Since its inception after Operation *Desert Storm*, the JTC has been a critical methodology for integrating fires with other joint functions to achieve military objectives. Codified in Joint Publication (JP) 3-60, *Joint Targeting*, the six-phased cycle facilitates deliberate and dynamic targeting, regardless of time constraints, and provides the flexibility to conduct some phases concurrently.¹ Unfortunately, its success in Operations *Enduring Freedom*, *Iraqi Freedom*,

Odyssey Dawn, and *Inherent Resolve* has led some commanders to adopt the JTC to integrate other joint functions—particularly information—during planning and operations. This misconception has caused serious challenges by conflating the information and fires domains and forcing the distinct information function into the confines of the phases and tempo of a targeting cycle intended to generate air tasking orders and fire support plans.

Below the threshold of armed conflict, the Department of Defense (DOD) must be prepared to support whole-of-government efforts or operate unilaterally to counter disinformation by influencing foreign individuals and populations.

Many information operations require the long-term, sustained delivery of strategic communications; others require immediate responses to inflammatory stories posted on social media platforms.² To

adequately integrate and synchronize the joint information function into *all* military operations, it is time to develop a Global Engagement Cycle (GEC) that will free information planners from the awkward and misaligned requirements of the JTC. This article proposes an expanded DOD definition for *engagement*, conceptualizes a new GEC for inclusion in joint doctrine, and argues for establishing a Joint Staff Global Engagement Division to lead the global integration of the joint information function into any military operation.

Defining Engagement

As U.S. competitors exploit the information domain to gain a competitive advantage over the United States and its allies, the need to integrate information-related capabilities (IRCs), including cyber and electromagnetic spectrum

assets, into the joint force continues to grow. Joint doctrine defines an *IRC* as a “tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.”³ The proliferation of *IRCs* enables potential adversaries to jam terrestrial communications and deny access to global positioning satellites that are critical for navigation, surveillance, and the delivery of precision munitions.

IRCs can also propagate disinformation through social media, seeding international doubt about the motives behind U.S. policies, the presence of forward-deployed U.S. forces, and the value of alliances, such as the North Atlantic Treaty Organization (NATO).⁴ Those who do not seek a direct confrontation with the United States, or who lack the conventional military means to achieve their objectives, will develop alternative methods to dominate through the information domain. This is evident in China’s current military strategy that directs the People’s Liberation Army to gain control of the “information sphere” and in the Russian defense strategy that requires its military forces to gain supremacy in any “information confrontation” that could occur in times of war or peace.⁵

In describing the seven joint functions, JP 3-0, *Joint Operations*, explains that a commander’s mission requirements will limit the use of the fires function, while the information function applies to all military operations.⁶ Although fires involve the use of lethal and nonlethal military force, the term *joint fires* does not include direct fire weapons because those systems fall under the joint function of movement and maneuver. The U.S. Army’s Fires Center of Excellence does not teach Soldiers how to employ Abrams tanks or Bradley fighting vehicles, nor does the U.S. Air Force Weapons School instruct future weapons officers on how to best position machine guns around an airbase. Rather, these schools provide curricula on indirect fires.

The preponderance of joint fires involves cannon and rocket artillery, precision munitions from aircraft, and missiles launched from naval vessels to

change the function of a target. While the dichotomy between direct and indirect fires appears evident, parsing which *IRCs* constitute joint fires can be nebulous. The best method for determining whether to categorize an *IRC* as a joint fires capability would be to confirm whether planners intend to use it to affect a target. Joint doctrine defines a *target* as an “entity or object that performs a function for the threat considered for possible engagement or other action.”⁷ With targeting enabling the joint force to prioritize targets and match the appropriate response to them, *IRCs* provide the flexibility to affect some targets without causing physical damage. For example, in lieu of influencing terrorists to surrender by destroying an Islamic State training camp with an artillery barrage, a commander might airdrop leaflets describing the overwhelming capabilities of coalition forces.

In other military operations, a commander may use *IRCs* to affect individuals and populations who *do not* perform a function for an adversary. Indeed, many information operations do not affect targets catalogued in the Defense Intelligence Agency’s Modernized Integrated Database (MIDB)—an extensive collection ranging from individual terrorists to chemical weapons production facilities to the order of battle for conventional forces. In Afghanistan, for example, the International Security Assistance Force (ISAF) would not classify a women’s rights organization in Kabul as a threat, yet coalition forces would still want to co-opt the activists to expand their efforts beyond the capital city to advance education and employment equality in rural areas. Without cataloguing the women’s group in the MIDB or adding a scheduled bilateral meeting to the air tasking order, the joint force still has a responsibility to synchronize this deliberate information operation with its other lines of effort and assess the outcome’s contribution to the commander’s desired endstate.

Outside of hostilities, information operations enable the joint force to engage with nonadversaries: in peacekeeping

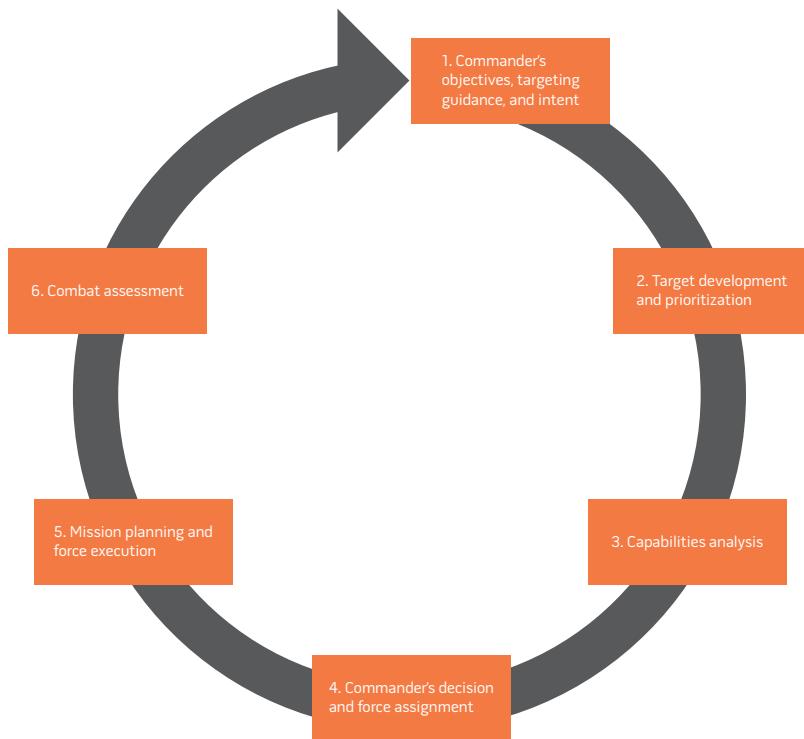
to influence a host-nation population to obey the rule of law, in humanitarian operations to inform internally displaced people where to find food and medical care, in peacetime to counter disinformation about U.S. troops stationed overseas. Unfortunately, the DOD dictionary limits the definition of *engagement* to “an attack against an air or missile threat [or] a tactical conflict, usually between opposing lower echelons maneuver forces.”⁸ Nonetheless, from the squad leader to the combatant commander, no Servicemember who receives an order to conduct a key leader engagement believes for a moment that he or she must carry out an assassination.

Some nonlethal engagements involve one-on-one dialogue based on preplanned messages to provide clarity and build trust during the conversation. Similarly, engaging the masses through press conferences and social media requires the development of talking points connected to strategic communications themes. This process depends on advanced planning to identify whom to engage, to craft meaningful messages intended to influence someone’s thinking or behavior, and to assess whether an engagement achieved the desired military endstate.

In light of the practical use of the word *engagement* by the joint force, it is time to expand the doctrinal definition of the term beyond its current lethal description by codifying a complementary nonlethal definition, as proposed here: “An attack against an air or missile threat; a tactical conflict, usually between opposing lower echelons maneuver forces; a nonlethal action, usually employing information-related capabilities, to influence the decisionmaking of an individual or audience not considered to be a threat at the present time.”

Introduction of this definition into joint doctrine would provide the joint force, at any echelon, with the flexibility to either employ *IRCs* in support of the joint fires function or retain them in a separate line of effort for the joint information function. The proposed nonlethal engagement terminology would clarify how information

Figure 1. The Joint Targeting Cycle from JP 3-60, *Joint Targeting*



operations could influence individuals and audiences not associated with an adversary, and the joint force would gain confidence in its ability to employ IRCs to support the achievement of operational and strategic objectives outside of the Joint Targeting Cycle.

The Limits of the JTC

Depending on the military operation, the tempo of the Joint Targeting Cycle can be too robust or, conversely, too slow to develop, execute, and assess nonlethal engagements. Information operations to deter disenfranchised youths from joining the Islamic State may take years, while a salacious allegation against U.S. forces posted on social media demands a response that cannot wait for the next day's Joint Targeting Coordination Board. Before outlining the proposed Global Engagement Cycle, it is worthwhile to consider why JTC requirements make that process problematic for synchronizing the nonlethal engagement line of effort for the joint force (see figure 1).

As with all other facets of the joint planning process, targeting begins upon receipt of the commander's guidance, including operational objectives, authorized actions against targets, and any delegated responsibilities for target validation and engagement. The commander's targeting guidance serves as the basis for selecting target systems and articulating desired effects to achieve an endstate. Targeting guidance does not always apply to information planners because of its focus on accomplishing a series of tactical tasks in one specific phase of a larger campaign. Typically, a staff publishes an execution order to achieve one objective and, while subordinate units initiate movement, the staff regroups to publish a fragmentary order with details for achieving the next objective. IRCs may contribute to accomplishing the immediate objective but other information operations require the commander to articulate strategic-level guidance for how to shape messages over the entirety of the campaign. Furthermore, the delegated target validation and engagement authorities may not apply to the employment of certain

IRCs, particularly special access cyber and electromagnetic spectrum programs requiring authorization from the President and/or Secretary of Defense.

Target development and prioritization incorporate a variety of intelligence disciplines to build target systems, their components, and individual targets. Entities validated as targets appear on the Joint Integrated Prioritized Target List (JIPTL), and advanced target development continues through the capabilities analysis phase of the Joint Targeting Cycle: mensuration of the target location (its latitude, longitude, and elevation), weaponeering calculations to match the best capability with the target, and a collateral damage estimation of potential lethal effects. Although essential for employing precision munitions, this capabilities analysis format is not conducive for determining how best to influence a diffused virtual audience through the information domain. Moreover, the limiting factor of target selection for nonlethal engagement remains the omission of nontarget entities from the JIPTL approved by the Joint Targeting Coordination Board. Information planners need an independent board to prioritize the individuals and groups who cannot be catalogued in the MIDB and to select the most appropriate IRCs to engage them.

In combat operations, the timing of the commander's decision to engage targets and assign forces to execute joint fires aligns with the battle rhythm to publish the daily air tasking order. In the Air Tasking Cycle, joint planners overlay targets from the JIPTL with available munitions and aircraft for a 24-hour period, which enables bomber and fighter squadrons to publish orders for mission execution. The need to publish an order early enough for forces to prepare for operations requires a disciplined staff process that drives the nomination and validation of targets for the next 48 and 72 hours.

Each 24-hour iteration of the Air Tasking Cycle serves a valuable purpose, but not for many of the deliberate shaping operations in the information domain, where it is unrealistic to

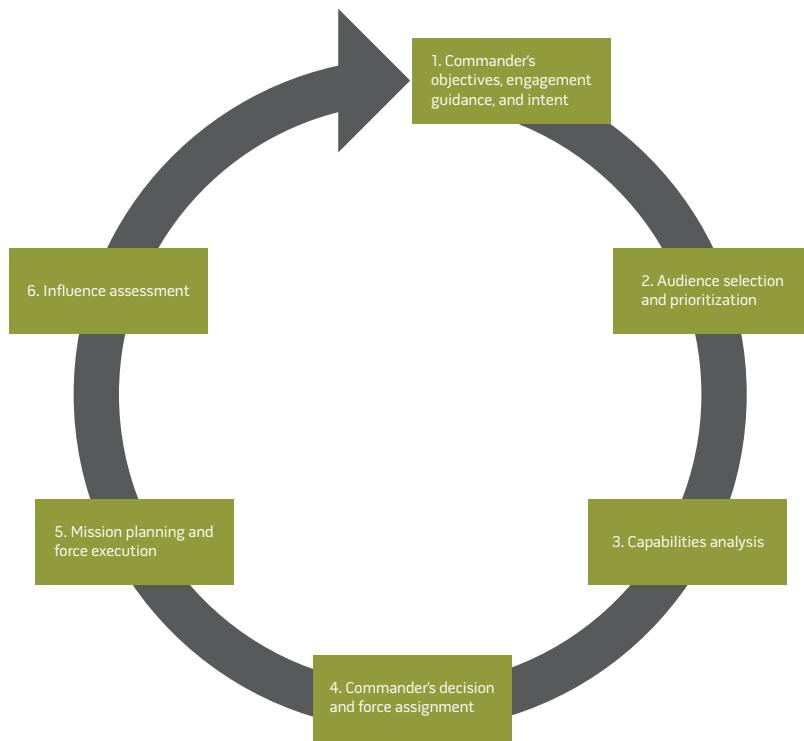
influence someone's thinking or behavior in just 1 day, or even 3. An IRC could momentarily deceive an adversary about the location of the joint force's main effort during a ground offensive, and that would constitute a joint fires task to achieve an effect on a specified target. However, when influencing Islamic State terrorists to surrender, nonlethal engagements may require months or years of sustained messaging through the employment of multiple IRCs before the joint force can observe a decrease in the number of voluntary fighters.

Assessing how well mission execution changed the function of a target will either complete the JTC or inform its next iteration. The combat assessment phase involves three specific steps: the intelligence analyst's battle damage assessment of physical and functional damage, the operator's munitions effectiveness assessment ("Did the weapon function properly?"), and, as required, the recommendation to reattack the target. As with capabilities analysis, the combat assessment phase can be problematic for information planners. Many nonlethal engagements are never intended to cause physical damage to a target or target system. Every information operation requires an assessment, but not one based on the 24-hour cycle that the Joint Targeting Coordination Board depends on to select new targets for the next day's air tasking order.

A New Global Engagement Cycle

The structure of the Joint Targeting Cycle provides a familiar and appropriate framework to design a new Global Engagement Cycle (see figure 2). Not intended to duplicate the established process for integrating joint fires, this proposed methodology would synchronize nonlethal engagements by requiring specific information function inputs from commanders, planners, and the joint force. By recognizing nonlethal engagements as a distinct line of effort, a headquarters could update its battle rhythm with the six phases of the GEC and establish working groups and coordination boards to select, validate, and prioritize audiences to engage with IRCs.

Figure 2. Proposed Global Engagement Cycle



To initiate the cycle, information planners would draft the commander's nonlethal engagement guidance to specify how to use the information function to support the joint force's short- and long-term objectives. This would ensure that the staff understands the commander's expectations for achieving certain tasks in the information domain during the current phase of the operation and what tasks would require the entirety of the campaign to accomplish. Both are critical for expectation management, as time constraints determine the frequency of working groups to develop audiences, decision boards to validate IRC employment, and assessments of mission execution. Engagement guidance should specify message themes to incorporate or avoid, especially when considering interagency or coalition partner information operations in the same operations area. Guidance should authorize IRCs for nonlethal use and delegate responsibilities for audience validation and engagement.

Similar to the electronic target folders created in the MIDB during target development, the GEC audience selection

and prioritization phase would provide planners with a standardized template for cataloguing individuals and groups for the joint force to consider influencing. The information operations community would need to develop a format for entries, identify an agency to maintain the database, and agree to who should have access to the material. Drawing from all-source intelligence, each entry should provide the name and location of an audience (individuals as well as groups), explain the audience's relationship to a larger population or social network, and identify its current opinions toward U.S. policy.

An individual audience could be the chief of defense forces for a country who is known to be the most trusted member of a prime minister's cabinet and who personally supports the presence of U.S. forces in his country. A group audience might transcend the boundaries of a geographic combatant command by including thousands of anonymous members of an Internet chatroom advocating for the dissolution of NATO. As mercurial as this type of audience may be, with

individual members joining and leaving the chatroom at any time, online forums remain viable groups for the joint force to influence in order to achieve a desired peacetime endstate to strengthen solidarity for the Alliance.

Capabilities analysis for nonlethal engagement involves two components: developing messages and selecting the best IRC to influence an audience. To prepare culturally suitable language that would gain credibility with an audience, message development requires collaboration among intelligence, information operations, public affairs, civil affairs, and legal specialists. Matching IRCs with an audience requires staff members to understand the capabilities available to the joint force, including special access cyber and electromagnetic spectrum assets.

Returning to the chief of defense forces example, the staff may determine that the best way to influence the individual would be for the U.S. geographic combatant commander to develop a personal relationship over a series of key leader engagements at conferences, office calls, and social events. Each engagement would require talking points to facilitate a dialogue intended to influence the defense chief's views on a specific topic. In contrast, an information campaign to deter disenfranchised youth from joining terrorist organizations may require multiple IRCs and minimal face-to-face conversation. For example, while an offensive cyber attack could shut down Boko Haram's recruitment Web site to prevent Nigerians from accessing it through their smartphones, a more effective means to influence youth in Chad could be radio broadcasts if Internet access is not as widely available in that country.

Once the commander authorizes a nonlethal engagement and assigns forces, subordinate units complete final preparations to employ IRCs. Joint targeting requires refinement of each target, and so should nonlethal engagement mission planning involve refinement of orders from a higher headquarters. Just as a joint terminal attack controller on the ground must verify a target location before requesting a pilot to drop a precision munition, determining how to engage

an audience must be refined at echelon. The joint force cannot deliver the same platitudes to the citizens of Venezuela and Syria and expect to achieve separate objectives for U.S. Southern Command (USSOUTHCOM) and U.S. Central Command (USCENTCOM). Rather, USSOUTHCOM planners must find ways to inform Venezuelans about the U.S. commitment to representative government, while USCENTCOM's staff needs to develop ways to deter Syrians from supporting the Islamic State.

The Tempo of Nonlethal Engagements

Engagement in the information domain cannot occur without an assessment through face-to-face conversation or the use of ISR assets to determine the audience's reaction to messages. When the commander's nonlethal engagement guidance includes a timeline for achieving objectives, the staff can synchronize collection assets required to assess how well an IRC influenced the thinking or behavior of an audience. Measures of effectiveness should be quantifiable, such as a decrease in the number of followers of an anti-NATO Twitter account, or an increase in favorable host-nation opinions of the presence of U.S. forces in their country.

By acknowledging that nonlethal engagement and assessment may take longer than a yearlong deployment to influence an audience (let alone the artificially accelerated tempo of a 2-week exercise), the staff should extend the assessment phase well past the traditional turnaround time required for the combat assessment of a precision munition strike against an adversary's chemical weapons production facility. Indeed, assessments in the information domain often depend on numerous intelligence sources monitoring the attitudes and behavior of an audience on multiple occasions, especially when determining the secondary and tertiary effects of a nonlethal engagement on a larger population or social network.

The Global Engagement Cycle would liberate information planners from the rigid 24-hour process critical for the timely publication of air tasking orders.

Adoption of the cycle would not exempt information planners from supporting the joint targeting process, since cyber, electromagnetic spectrum, and information operations specialists must continue to participate in target development working groups and Joint Targeting Coordination Boards to explain how IRCs could achieve desired effects on targets. However, the commander must provide information planners with the flexibility to develop audiences and assess nonlethal engagements over an entire military campaign and in peacetime. Instilling confidence in a strategic approach to nonlethal engagement would help to change the current DOD culture that instinctively associates the information function with the fast-paced planning, execution, and assessment of joint fires.

While the desire to influence an audience's thinking or behavior may involve years of nonlethal engagements and assessments, many scenarios necessitate a response from the joint force within 24 hours. Information planners should consider ways to conduct dynamic nonlethal engagements by conducting some phases of the Global Engagement Cycle concurrently or external to established decision boards. Although nonlethal engagement may start within minutes of the release of a fake story on the Internet, the staff must apply the GEC dynamically to select appropriate audiences, develop coherent messages tied to strategic communications themes, assign IRCs for mission execution, and articulate measures of effectiveness for the post-engagement assessment.

For example, an anonymous report on WhatsApp that falsely accuses the U.S. Air Force of killing dozens of civilians in an airstrike on a Kandahar hospital is likely to elicit an emotional international outcry, especially if the account includes gruesome photos of deceased women and children. To prevent a violent mob from attacking the U.S. Embassy in Kabul and protect U.S. military advisors operating across the country, ISAF cannot wait for the next day to respond. Available capabilities to refute this disinformation may involve coordinating

with social media companies to remove a viral post from their platform, a counter-cyberattack against the online profile of the originator of the story, sharing intelligence about the hospital with city leaders in Kandahar, or a robust public affairs presence through social media and press conferences.

A Global Integrator for Information

Due to IRCS' reach beyond regional boundaries, it is no longer feasible to rely on each combatant command to synchronize its own nonlethal engagement in isolation from one another. As Peter Singer and Emerson Brooking argue in *LikeWar: The Weaponization of Social Media*, competitors in the information domain have already influenced international opinions and values formerly taken for granted. Computer bots generate fake news stories on popular blogs, and offices filled with state-funded trolls malign public figures in other countries by derailing conversations in reputable chatrooms.⁹

From questioning who shot down a Malaysian airliner over Ukraine in 2014 to influencing public discourse in another country's democratic elections, the ubiquity of disinformation has sown doubt in traditional democratic norms, news sources, national governments, and alliances. Countering these challenges before the next armed conflict erupts depends on implementing a Global Engagement Cycle to establish credibility with foreign audiences in advance, so that those same audiences would be more trusting of U.S. and coalition information sources before the cacophony of disinformation grows exponentially.

As combatant commands reorganize their staff and battle rhythm to better integrate the joint information function, they will turn to the Joint Staff for cross-geographic and cross-functional command integration. In 2018, the Secretary of Defense designated the Chairman of the Joint Chiefs of Staff (CJCS) as the Global Integrator, responsible for "the arrangement of cohesive Joint Force actions in time, space, and purpose, executed as a whole to address

trans-regional, multi-functional challenges across all domains."¹⁰ Within the Joint Staff Directorate for Intelligence (J2), the Targeting Division serves as the global integrator for joint targeting. This includes writing national targeting policy, federating target development between combatant commands and the Intelligence Community, and recommending enterprise-wide solutions to share target material. In contrast, when it comes to the joint information function, the Joint Staff Directorate for Operations (J3) does not possess a comparable division resourced to serve as the global integrator of nonlethal engagements.

Consider the success of Russia's information campaign directed toward Estonia in influencing a significant portion of the Russian-speaking minority to believe they are marginalized within the country. Polling indicates that some who trust Russia's RT and Radio Sputnik as credible news sources question the value of the European Union in improving their quality of life and believe that Estonia has more in common with the Russian Federation than NATO.¹¹ In response, the commander of U.S. European Command (USEUCOM) could direct his staff to develop a counterinformation campaign to bolster Estonian support for NATO. However, the geographic combatant command could not do this alone, and its staff should be able to turn to the Joint Staff for assistance in coordinating nonlethal engagement efforts with functional commands and interagency partners.

While USEUCOM could collaborate directly with the U.S. Embassy in Estonia, the Joint Staff is better situated to involve other parts of the Department of State in the planning process—namely, the Global Engagement Center and the Bureau of European and Eurasian Affairs. In addition to liaising with Intelligence Community partners that possess unique insight into the political, social, and economic systems in Estonia, the Department of Energy's Oak Ridge National Laboratory studies the population densities of urban areas around the world, which could shape where the joint force directs its nonlethal engagements.

Should USEUCOM choose to use broadcasting or social media to influence Russian-speaking Estonians, the Joint Staff could collaborate with the U.S. Agency for Global Media, since this non-DOD entity may be better positioned to engage appropriate audiences through Voice of America's Russian-language service, the Polygraph.info fact-checking Web site, and Current Time TV.

A New Global Engagement Division

If the Joint Staff J3 established a Global Engagement Division, it would not only serve as the interlocutor between the combatant commands and interagency partners but also integrate the commands' collective efforts to achieve a common endstate. The division could ensure that functional commands, such as U.S. Cyber Command (USCYBERCOM), do not develop audiences or conduct nonlethal engagements without synchronizing with the appropriate geographic command. Not only would this reduce staff work by ensuring that commands share their products with one another, but it also would prevent "information fratricide." This form of fratricide might involve USCYBERCOM shutting down a Web site in Estonia without realizing that a USEUCOM public affairs officer was actively participating on the site by posting favorable stories about NATO partnership exercises in the Baltic states.

To accomplish this level of integration, the CJCS should consider resourcing the Deputy Directorate for Global Operations J39 to establish a new Global Engagement Division. To function as the global integrator for nonlethal engagements crossing geographic boundaries and functional domains, the division could organize into three branches: operations and plans, automation, and doctrine and policy.

The most robust branch would need to be operations and plans, with each action officer assigned a combatant command portfolio. By participating via video teleconference in working groups and decision boards with the command's information planners, the

Joint Staff representative could clarify supported and supporting command roles for developing nonlethal engagements toward specific audiences. When a commander's objective or the complexity of an information campaign exceeds the capacity of one command to plan and execute, the Joint Staff action officer could recommend ways to federate audience and message development with other DOD components or advocate for allocating additional interagency or coalition partner IRCs to support nonlethal engagements.

For the operations and plans branch to serve a decisive role in advancing global integration, it would depend on the automation branch developing new computer applications or integrating into existing knowledge management systems. The MIDB for target entities provides a standard electronic target folder for every catalogued entity, and the automation branch might consider how the joint force would want to build and manage a national-level database of individual and group audiences for potential nonlethal engagement by any command.

Applying these future automation systems would require new joint doctrine—not only an expanded definition of engagement but also technical details about how to conduct the six phases of the Global Engagement Cycle. The doctrine and policy branch could lead the development of new CJCS instructions and manuals to codify how to select and develop audiences, the dichotomy between IRCs used in joint targeting versus nonlethal engagement, and post-engagement assessment standards. Not only could this branch update these documents based on extant practice, but it also could advocate on behalf of the nonlethal engagement community during Joint Staff-led revisions of overarching joint publications, including JP 5-0, *Joint Planning*, JP 3-0, *Joint Operations*, JP 3-12, *Cyberspace Operations*, and JP 3-13, *Information Operations*.

A Distinct Approach for Nonlethal Engagement

When the Secretary of Defense established information as the seventh joint

function in 2017, he directed DOD to consider the implications across doctrine, organizations, education, and personnel.¹² An expanded joint definition of engagement would allow commanders and planners to reframe how they develop and achieve nonlethal effects. Adopting the Global Engagement Cycle as an alternative to the Joint Targeting Cycle would provide a greatly needed methodology to address current inadequacies with how the joint force integrates the information function into all military operations. Information planners and IRCs remain critical to the Joint Targeting Cycle, but efforts to influence the thinking and behavior of nonadversarial audiences require a separate process to counter the revisionist powers and rogue regimes competing with the United States and its allies across all dimensions of power.

The joint force must build credibility with audiences in foreign countries before hostilities or crises arise, as U.S. competitors have already begun to aggressively engage in duplicitous and subtle ways to shape the information domain, short of armed conflict. USCYBERCOM will develop means to prevent near-peer competitors from dominating the information domain during named operations and crises. Geographic combatant commands will develop influence strategies as well, but they cannot develop a strategy in isolation. Countering Russian disinformation no longer remains USEUCOM's challenge exclusively, and violent extremist organizations recruit new terrorists from within U.S. Indo-Pacific Command's boundaries to conduct attacks within USCENTCOM's operations area and against the homeland. Just as the George W. Bush administration established the Office of the Director of National Intelligence to improve intelligence-sharing after 9/11, the joint force would benefit greatly from the Joint Staff establishing a Global Engagement Division to enhance collaboration between combatant commands and interagency partners. Investing in the integration and synchronization of non-lethal engagement efforts today helps to achieve national security objectives before

the joint force must resort to placing Servicemembers in harm's way. JFQ

Notes

¹ Joint Publication (JP) 3-60, *Joint Targeting* (Washington, DC: The Joint Staff, September 28, 2018), II-3.

² Gregory M. Tomlin, "#SocialMediaMatters: Lessons Learned from Exercise Trident Juncture," *Joint Force Quarterly* 82 (3rd Quarter 2016).

³ JP 3-13, *Information Operations* (Washington, DC: The Joint Staff, November 20, 2014).

⁴ "Special Edition: Countering Russian Propaganda," *Per Concordiam: Journal of European Security and Defense Issues* 7 (2016).

⁵ *Challenges to Security in Space* (Washington, DC: Defense Intelligence Agency, January 2019), 14, 29, available at <www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf>.

⁶ JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, October 22, 2018), III-1.

⁷ JP 3-60.

⁸ JP 3-0 and JP 3-01, *Countering Air and Missile Threats* (Washington, DC: The Joint Staff, May 2, 2018).

⁹ P.W. Singer and Emerson T. Brooking, *Like War: The Weaponization of Social Media* (Boston: Houghton, Mifflin, Harcourt, 2018).

¹⁰ Jim Garamone, "Global Integration Seeks to Buy Leaders Decision Time, Increase 'Speed of Relevance,'" Defense Media Activity, July 2, 2018.

¹¹ Mridvika Sahajpal, Silviu Kondan, and David J. Trimbach, "Integration Policy & Perceptions in Estonia," *Foreign Policy Research Institute Baltic Bulletin*, May 7, 2018.

¹² James Mattis, Department of Defense memorandum, "Information as a Joint Function," September 15, 2017.



Detention Operations as a Strategic Consideration

By John F. Hussey

In major conflicts dating back to World War II and continuing through recent operations in Iraq and Afghanistan, military planners have not conducted the necessary planning and logistical support with regard to enemy prisoners of war (EPWs) and detainee operations (DO). Many current military and political leaders believe that the United States did not conduct

detention operations correctly in Afghanistan, Iraq, and at Guantánamo Bay. This has resulted in tactical-level failures that have had significant operational- and strategic-level impacts on the conduct of military operations. It is time to change this paradigm and no longer treat EPW operations and DO as an afterthought.

The U.S. military continues to make errors in the vitally important mission of DO and has reduced its ability to achieve national objectives and, in some cases, created international embarrassments. If we do not place significant emphasis on

this critical aspect of planning, the same mistakes will be repeated, and the U.S. military will lose its credibility, both domestically and internationally. Moreover, if these mistakes are not rectified, the Nation could fail in the other phases of combat operations. This article thus conveys historical examples of insufficient and ineffective planning for DO and how these deficiencies have tarnished the joint force. The article also provides recommendations to future planners that may reduce errors in DO, thus avoiding awkwardness and assisting in achieving both military and national objectives.

Major General John F. Hussey, USAR, is the Commanding General of the 200th Military Police Command, U.S. Army Reserve.

Let us begin by defining who a *détainee* actually is. It can be any person captured, detained, or otherwise under the control of Department of Defense (DOD) personnel. An EPW is categorized as a *belligerent*, which is defined as a person who is engaged in hostilities against the United States or its multinational partners during an armed conflict.¹ A belligerent is classified under the umbrella term of detainee.

Presently, the National Defense Strategy outlines an approach that names Russia and China, North Korea and Iran, and violent extremist organizations (the so-called 2+2+1 strategy) as potential engagements that the U.S. military may confront in the near future. We will likely face a complex global security environment involving near-peer competition that includes massive combat formation unparalleled since World War II or the Korean War. We can also expect that these conflicts may devolve into a hybrid type warfare with any of the nations noted, which means that American forces will be dealing with some form of insurgency. Despite clear guidance provided by the President, Secretary of Defense, and Chairman of the Joint Chiefs of Staff in various strategy documents, how much thought and planning have combatant command (CCMD) staffs given to DO in the area of operations that we may engage in?

Background

The Korean War is perhaps most emblematic of the devastating effects that may result due to inattention to the DO part of an overall plan. The Korean War EPW plan highlights many of the errors that the United States made in this operation and failed to learn in subsequent operations. Initially, the Army identified Pusan, a port city on the southeast portion of the Korean Peninsula, as the holding area for captured North Korean forces. By August 1950, the United States and its allies had captured approximately 1,900 prisoners. General Douglas MacArthur conducted his famous Inchon landing on September 15, 1950. The landing at Inchon cut the North Korean lines of communication and routed the North Korean military. Consequently,

over half a million North Korean forces were caught between MacArthur's landing force and the U.S. 8th Army that had been pushed to the southern tip of the peninsula. As the fighting mounted, coalition forces were left with over 176,000 North Korean EPWs by the end of October 1950.² While this may have been good news for the land component commander, there was also a dark side in that there was simply no plan to handle so many prisoners. EPW operations were an afterthought. In the end, the EPW camp on Geoje Island was "born of expediency."³

Unlike previous wars, the North Koreans mounted a strategic-level campaign to continue the war within the camp. Several North Korean senior leaders allowed themselves to be caught with the sole intent of going into the EPW camps, rallying the forces, and causing strategic-level embarrassment for U.S. and South Korean forces. For instance, Colonel Lee Hak Ku surrendered on his own volition. He left his unit in the mountains and approached the American lines at night with the sole purpose of being captured.⁴ Lee played a prominent role as a senior leader within the camps and was the EPW spokesman in the riot and hostage-taking that occurred there. The highest leaders within the Communist Party of North Korea candidly admitted that they planned for the covert infiltration of agents into the prison camp at Geoje-do for the express purposes of "masterminding incidents within the United Nations Command [UNC] prisoners of war camps."⁵

As part of the North Korean strategic plan, prisoners rioted in Geoje-do in May of 1952. This rioting created a dilemma for the guards and senior leaders of the camp. In response, Brigadier General Francis T. Dodd decided to enter the camp in an effort to mitigate the disturbances. Shortly thereafter, Dodd was taken hostage and held for approximately 80 hours. During this arduous time, Brigadier General Charles Colson was in charge of camp operations. In his haste to secure the release of a fellow general officer, he signed documents prepared by the Chinese and North Korean EPWs. Dodd

also signed the same documents titled "Korean-Chinese Prisoners' Grievances to the World" and "UNC POW [prisoner of war] Camp Affidavits."⁶ These documents, in essence, gave the impression to the international community that the U.S. military was not treating EPWs humanely and thus resulted in the United States losing legitimacy on the international stage.

Based on American actions within the operation, and including what many deemed to be unnecessary violence, the United States received condemnation in the British and American media. An editor from a magazine in Moscow compared Geoje Island to Maidenek and Dachau, both Nazi death camps.⁷ Over the period of 3 years, there had been a total of at least 14 leaders, and the camp became known as "the graveyard of commanders."⁸ Both Dodd and Colson were relieved from their duties at Geoje-do and reduced in rank to colonel.

The following comments were made by senior military and political leaders describing DO during the Korean War.⁹ They demonstrate that DO has been problematic for the U.S. military for an extended period of time. More concerning is the fact that military planners have failed to appreciate the gravity and depth of the DO mission and have also failed to study the lessons of past conflicts and the importance of proper planning for this strategic mission.

- UN Commander General Mark Clark, USA, referred to the situation in which Dodd was taken hostage at Geoje-do as "the biggest flap of the war."¹⁰
- Secretary of the Army Frank Pace, Jr., chastised Colson for making "misleading and embarrassing" concessions to the POWs to secure Dodd's release. These same signed confessions were used by the enemy against the United States in the media and at the peace settlement talks.¹¹
- Senator Styles Bridges made a press statement describing Dodd's performance during the hostage incident as "stupidity" and threatened an immediate Armed Services subcommittee investigation.¹²

- Vice Admiral C. Turner Joy, senior UN delegate to the truce talks at Panmunjom, stated, “I’m certainly going to take a beating over this at the conference table.”¹³ He was referring to his continued dialogue with the North Koreans and Chinese during peace settlement talks to end the war.

The failure to plan for and conduct DO correctly in Iraq is similar to the failures at Geoje Island. I spoke to a fellow officer who was assigned to the Military Police (MP) brigade responsible for theater-level DO during the initial invasion. I asked him a simple but pointed question regarding DO: “What really went wrong?” He told me that there was no DO plan and that when he pressed higher headquarters for answers on what to do, he was told to “Figure it out, major.” A major can figure out where to put the sally port on a detention facility or what time meals should be served. However, a major does not have the authority and, therefore, cannot order certain assets such as an Engineering brigade to construct and set up more camps in theater. A major cannot requisition additional MP brigades and MP battalions into theater, nor can he figure out a method to replace Army Reserve and National Guard Soldiers who were wounded or went home based on their orders terminating in accordance with their mobilization time. These are decisions at a much more senior level and should be part of a well-coordinated DO plan.

So what really did happen at Abu Ghraib? There was a failure to plan for DO at all levels. At the operational level of war, the proper command and control (C2) element was never considered. This failure resulted in facilities not being properly resourced, maintained, and manned. Perhaps just as important was the fact that the MP units assigned to the DO mission were not a high priority. Therefore, they were not placed high on the time-phased force deployment data list (TPFDL) and, as a result, arrived in theater late, and in many cases their personnel and equipment arrived scattered.¹⁴ The failure to provide an overall commander of DO with C2 authorities over



Marine with Combined Anti-Armor Team 1, 1st Battalion, 5th Marine Regiment, escort enemy prisoner of war away for questioning after discovering illegal drugs and improvised explosive device-making material, Helmand Province, Afghanistan, October 19, 2009 (U.S. Marine Corps/John McCall)

all detention facilities allowed for the MP and Military Intelligence (MI) missions to cross barriers and come into conflict, thereby creating ambiguity, most particularly in who was actually in charge.

At the tactical level, Soldiers were not trained properly at mobilization platforms, and there were no standard operating procedures within the camp. There was a mix of uniformed personnel interacting with contractors, and little oversight of either. The Geneva Conventions were routinely violated, and much of the day-to-day care and custody of the prisoners was abdicated to MI personnel and contractors. All these issues were contributing factors that led to the abuse. Many of these issues could have been avoided if the DO plan had been appropriately staffed and a proper

C2 element planned and resourced. The failures at Abu Ghraib also resulted in the loss of U.S. credibility at home and on the international stage.¹⁵

The American DO plan for Afghanistan suffered flawed planning as well. There were no trained DO units in theater at the onset of the war. While this is understandable based on the various aspects of the plan, nevertheless it had consequences. Over 3,500 Taliban surrendered in the Kunduz area and were under the control of the Northern Alliance at a prison in Mazar-e-Sharif. Riots ensued in which detainees overpowered untrained guards. The prison had to be retaken by force, resulting in the death and injury of U.S. and allied personnel. Additionally, over 500 detainees were killed.¹⁶ There were allegations



Jordan Armed Forces–Arab Army Quick Reaction Force Female Engagement Team member practices physical search procedures on U.S. Marine with 11th Marine Expeditionary Unit Female Engagement Team during detainee operations in Jordan, August 5, 2019 (U.S. Army/Shaiyla B. Hakeem)

that the Northern Alliance abused detainees and that maltreatment resulted in unnecessary death. Some tried to link this debacle to the U.S. military.

U.S. policy dictated that captured al Qaeda prisoners were not covered by the Geneva Conventions and were referred to as “detainees.” Although afforded many of the same rights and privileges as EPWs, the treatment they received in Afghanistan and at Guantánamo Bay—and the reported cases of abuse—has resulted in increased international scrutiny. Questions began to surface regarding the treatment standards of detainees, and much of the debate centered on the appropriate classification of captured Taliban and al Qaeda fighters and what, if any, legal status they held.¹⁷ Planners never considered the legal authority to detain individuals captured on the battlefield, nor did they discuss the standard of treatment that a detainee should receive.

The failure to successfully conduct DO in the Korean War led to the relief of senior officers involved. Not surprisingly, the same results occurred in Iraq. The calamity at Abu Ghraib resulted in the end of two general officers’ careers. Consider that Defense Secretary Donald Rumsfeld found that Lieutenant General Ricardo Sanchez had been derelict in overseeing detention in Iraq. Many speculate that the mistreatment of detainees at Abu Ghraib resulted in Sanchez not being nominated for his fourth star.¹⁸ Brigadier General Janis Karpinski, who oversaw DO at Abu Ghraib, was reprimanded, relieved of her command, and demoted to colonel.¹⁹ Presently, the detainee situation from the war in Afghanistan remains unresolved, with some 40 detainees remaining in custody at Guantánamo Bay.

Crunching the Numbers

The historical examples cited should motivate planners to give DO the neces-

sary consideration that any aspect of an operational plan deserves. DO simply cannot be a “hand-wave,” that is, a non-issue deemed as unimportant and glossed over. The following provides staffs with various considerations when planning for theater-level DO.

Initially, staffs need to ask the right questions when wargaming for DO. They must plan to avoid many of the pitfalls that have been detrimental to commanders and senior leaders in past conflicts. According to a RAND study, the U.S. military does not plan well for DO, and as a result it has been hampered by failures in this part of the campaign planning.²⁰ It is time to reevaluate the concept of operations and the DO portion of a plan. More than likely, in the past, some lead mid-grade officer sat in a room, drew up a plan either individually or with a small group of personnel operating in a vacuum with no oversight or staff input, and never synchronized the

Table 1. Detainee Operations Projections in a 2+2+1 Strategy

Country	Number of active-duty troops	Number of reserve troops	Total troop strength
China	2,183,000	510,000	2,693,000
Russia	1,013,628	2,572,500	3,586,128
North Korea	945,000	5,500,000	6,445,000
Iran	534,000	400,000	934,000
Estimated number of active Salafi-Jihadist fighters	100,000–230,000	Not applicable	100,000–230,000

(The number of troops used for the projections was provided by Global Firepower.¹ The projections for Salafi-Jihadist Fighters was provided by a report from Dr. Jones.)

Notes

¹ Global Firepower, available at <<https://www.globalfirepower.com/countries-listing.asp>>.

² Seth G. Jones et al., *The Evolution of the Salafi-Jihadist Threat: Current and Future Challenges from the Islamic State, Al-Qaeda, and Other Groups* (Washington, DC: Center for Strategic and International Studies, 2018), available at <www.csis.org/analysis/evolution-salafi-jihadist-threat>.

plan with other staff members. It is time to lay the plan out, set aside the time for the staff to review it, and actually put it to some type of exercise.

Before an exercise is scheduled, we must ask whether the courses of action are adequate, feasible, and acceptable. The plan needs to be staffed and vetted and, if possible, exercised through some form of a simulation to test its effectiveness. Important questions need to be asked, such as what is the actual movement plan for detainees. Suppose the concept of moving detainees is by ground or air. If the number is 75,000 detainees, for example, how many vehicles or airplanes will that require? How much fuel will be consumed? How much crew rest will be involved for movements? While the MP mid-grade officer will have this concept all planned out, does the Joint Forces Air Component Commander or Joint Forces Land Component Commander (JFLCC) know his or her assets are part of a DO plan? Much of this will occur during Phase III operations, when combat is expected to be at its most brutal state. This is not the time to discover that air assets, vehicle assets, and main supply routes are unavailable for the movement of detainees.

In addition, if detainees are not moved back to the rear, combat arms personnel will be obligated to guard detainees and thus cannot exploit enemy weaknesses and vulnerabilities. This will limit U.S. and allied forces' ability to advance, and consolidated gains in large-scale contingency operations may be vulnerable to an enemy

counterattack or acts of insurgency by hybrid type operatives.

Perhaps the most important question that a staff must contemplate when planning for DO is how many troops does each of the potential U.S. opponents actually have. Table 1 depicts the potential adversaries troop numbers in the 2+2+1 strategy.

During World War I, the number of EPWs as a percentage of the total force mobilized was 9.8. Of their total force mobilized, the Allies experienced a capture rate of 8.5 percent, while the Central Powers experienced a 12 percent rate of capture of total mobilized forces. During World War II, the number of EPWs as a percentage of the total force mobilized was 29.²¹ The Allies had approximately 23 percent of their forces captured, while the Axis had approximately 37 percent of their forces captured. In terms of raw numbers, German EPWs were approximately 11,094,000.²² Planners underestimated the number of prisoners the Allies would take and the speed at which they would take them. By June 1945, the United States held more than 425,000 POWs who lived in camps throughout the Nation. After the Normandy invasion, the United States was receiving 30,000 POWs per month, and during the last months of World War II, the numbers soared to 60,000 per month.²³ During the Korean War, the allies captured up to 200,000 North Korean and Chinese prisoners. During Operation *Desert Storm*, the 800th MP Brigade processed and interned 69,822.²⁴

In Iraq, over 160,000 detainees were processed through U.S. DO camps.²⁵

It is extremely difficult to predict how many EPWs will be taken during any conflict. With more lethality in warfare, these numbers may trend downward; however, staffs must plan for a worst-case scenario. The numbers above reflect historical data from various wars that the United States has been engaged in. Considering the 2+2+1 strategy, the percentages of EPWs captured was based on 5 percent and 10 percent, just to provide military planners a figure to demonstrate the vast number of EPWs who may inhabit a camp. This should immediately draw the attention of various staff members regarding screening, transport, interrogation, feeding, preventive medication and care, and custody. Table 2 depicts the concept of the 2+2+1 strategy as it relates to EPWs, with projected capture rates of 5 percent and 10 percent.

The combatant commander (CCDR) and JFLCC must also be concerned about the quantity and quality of tactical-level personnel involved in the DO mission. Both in Korea and DO post-9/11, the U.S. military was faced with a variety of challenges, including a lack of qualified personnel, personnel who had not planned properly, officers who did not forecast and plan for the massive numbers of prisoners, and the inability to correctly identify the detainee populations. One of the first considerations is numbers. Doctrinally speaking, an MP detention battalion is typically organized to support, safeguard, account for, guard,

Table 2. The 2+2+1 Strategy as It Relates to EPW

Country	Number of active-duty troops	Number of reserve troops	Total troop strength	Number of total estimated EPWs based on 5 percent	Number of total estimated EPWs based on 10 percent
China	2,183,000	510,000	2,693,000	134,650	269,300
Russia	1,013,628	2,572,500	3,586,128	179,306	358,612
North Korea	945,000	5,500,000	6,445,000	322,250	644,500
Iran	534,000	400,000	934,000	46,700	93,400
Estimated number of active Salafi-Jihadist fighters	100,000–230,000	Not applicable	100,000–230,000	5,000–11,500	10,000–23,000

and provide humane treatment for up to 4,000 detainees; however, certain missions may require additional resources and manning.²⁶ The requirements regarding personnel, materiel, and logistical issues are immense.

The U.S. military may be engaged in a conflict for an extended period of time and will not have the capacity to rotate formations and still meet the requirements. In Iraq, the MP corps had to take Soldiers from other military occupational skills and train them to be the guard force within its camps. On occasion, other Services provided troops to serve as guards in DO facilities. Lastly, consider that many of these assets reside in the National Guard and Army Reserve and have not had training to prepare for the care, custody, and control of 4,000 detainees. The number of potential EPWs will, in turn, require greater attention from the CCDR and JFLCC as to the quality and quantity of tactical-level personnel. This may also require that National Guard and Army Reserve DO planners are involved in the planning prior to battle and it may require an adjustment to the TPFDL to ensure the correct DO assets to support the plan are in theater prior to the start of Phase III operations.

Moreover, the U.S. military lacks sufficient language skills capacity to cover the 2+2+1 scenario. Each of the nations listed in table 2 has numerous dialects that planners must account for. For example, there are seven Chinese dialect groups, with the predominant being Mandarin from the north/southwest areas of the country. This dialect comprises approximately 72 percent of the population. Although Russia is vast in geographical landscape, it basically

has three groups of dialects: northern, southern, and central, with the latter heavily influenced by the other two. The official language of Iran is Persian (Farsi); however, seven more languages are recognized as regional languages. In North Korea, U.S. forces can expect three different dialects spoken by forces there. Two are spoken by residents of Pyongyang, thus indicating a potential for being in the inner circle of North Korean politics. This is extremely important for the interrogators who may be targeting these individuals as high-value detainees and for the housing of North Korean detainees. Regarding various terrorists who may be captured, there are an array of languages that these individuals may speak. U.S. military interpreters are divided into categories based on citizenship and clearances. While it is important to have these individuals to conduct DO, there will be a need for MI to have interpreters of similar language capabilities present to conduct interrogations and exploit captured materials, including computer hard drives that will be in a foreign language. Does the DO plan account for this? Are contracts identified and payment ready to proceed in the event of ground conflict? How fast can and will these interpreters arrive in theater? How will they be cleared and how long will that take to do so?

Additional Tactical Considerations for Staff Planning

Prior to the processing of detainees, commanders and their staffs have a variety of issues and conditions to think about. One consideration is the actual location of the camps that will be used

throughout the area of operations. Camp location and construction are of significant importance. In Iraq, the camps were large enclosures surrounded by wire. This was similar to Geoje-do. The MP guard force could not enter the camp with great ease and, therefore, they often avoided entering the camps at all. This ceded control of the camps to the detainees. The detainees used rocks found in the camps as weapons to throw at guards. In some instances, the end result was lethal force being used against detainees. In both Camp Bucca and Abu Ghraib, detainees took advantage of the inability of the guard force to penetrate into the compounds and began to tunnel out. This may be addressed by reversing an expeditionary mindset and building a structure that can prevent such problems.

The prison complex in Afghanistan cost a great deal more money than other ones; however, there were fewer riots. With the right construction and efficiencies built in, the guard force can be reduced because it had control of the facility. Although U.S. forces may be expeditionary, these camps are functioning for several years, so they are not really expeditionary. Small camp compounds provide better guard force control. Construction should include concrete pads to prevent tunneling and improvised weapons availability to detainees. Divide camp areas into smaller communal cells. Provide individual segregation cells for high-value detainees who are being interviewed by military intelligence, investigators, and other assets. The segregation cells will also serve to house those detainees not in compliance with camp rules. The forward edge of combat areas

is subject to change; the chief of staff at each CCMD should ensure that camp locations can adapt to geographical limitations that may affect flow of detainees, materials, and personnel in support of camp operations. The camp locations and detainee flow must be compatible with the overall plan and ensure that there are ample air and land assets available to move detainees without affecting Phase III operations.

The plan must also include provisions for appropriate medical care within the camp. The overall footprint of the camp should be considered because detainees will have to be moved both to interrogations and to medical appointments. In addition, they may have to be transported to civilian courts. If the camp is large, movements will be complex and often require multiple simultaneous movements resulting in a larger guard force requirement. Is the camp near an airfield if air operations are part of the overall plan? What is the road structure in and around the potential camp location? If the location is near an urban area, it may offer enemy forces surrounding higher terrain that will allow for observation and enemy attacks on the facility. Will the location of the camp be compatible with the necessary access to support both Secret Internet Protocol Router Network and Nonclassified Internet Protocol Router Network? Does the environment support a camp structure—that is, will it flood during the rainy season or will the metal facilities rust prematurely based on environmental impacts? Engineer assets must be robust to repair infrastructure destroyed by detainees who will keep the “war” going on within the camp. They will also be needed for routine maintenance, normal wear and tear on infrastructure, and expanding structures within the camp or building new structures based on new requirements.

Geoje-do had approximately 138,000 EPWs. Logistics considerations included feeding a large population three times daily, and sanitation facilities must be a contributing factor to camp design. The culture of the detainees must also be taken into consideration during the design of a DO camp. In *Desert Storm* the

U.S. military built wooden commodes for the EPWs to use. In the Middle East, they do not defecate by sitting on a commode; rather, they squat over a hole in the ground. The EPWs literally stood on the commode and defecated on the wall behind them, thus raising sanitation concerns. Even the color of prison garments must be considered. In Geoje-do, each prisoner was issued a summer uniform of bright red, thus delighting the Chinese communists who believed that red symbolized good luck and health. Conversely, the uniform selection angered the Koreans, both communist and noncommunist, who associated the red uniform with the Japanese occupiers of World War II. The Japanese issued red uniforms to those prisoners condemned to death. Orange jumpsuits seemed to anger many of the militant leaders in the Middle East. This was the same jumpsuit used by American forces who housed detainees at Guantánamo Bay. Terrorist organizations in Iraq, as well as the so-called Islamic State, placed individuals into orange jumpsuits prior to their beheadings.

The DO plan must take into consideration the political or religious ideologies of those being detained by U.S. military forces. The inability to predict insurrection within the confines of the prison will lead to continued violence and injuries among the detainee population as well as the guard force. The failure to observe and interpret detainee behavior through subjective indicators such as will, motivation, morale, health, and welfare are all elements that will affect the atmospherics within the camp and directly correlate into the size of the guard force and the housing of particular detainees.

Many have suggested that detention facilities in both Iraq and Afghanistan served as recruiting and training grounds for insurgents and terrorists.²⁷ It is widely accepted that high-value detainees should not be housed with “common criminals.” A threat assessment must be developed for each detainee that considers the variances in radicalization, seniority within the military or political structure, and experience and standing among those labeled as a high-value detainees. Planners must consider how to assess the nature of

incoming detainees and tailor detention experiences accordingly. More specifically, when and where practical, captured unit information and available intelligence data should be used to broadly classify detainees on a limited number of characteristics, perhaps including political indoctrination, radicalization, seniority, experience, and education and/or work skills.

Once classified, the detainees should be placed in a facility that has been adequately configured to segregate those considered to be less radicalized. Segregating and housing detainees on the lower end of any of these trait scales with those on the higher end risks facilitating substantial indoctrination and training in a detention facility. This would also hold true for nations that have an authoritarian type structure. It would be best not to house common soldiers with senior leaders within the military who are also part of the political establishment that we may be in conflict with. Remember, the Eastern way of war is far different from the Western way of war, and that also holds true in DO. Finally, it is imperative to have the correct number of screened and trained linguists identified and ready to perform the mission. In many instances, U.S. personnel are uneducated on the culture of the detainee populations, and therefore a cultural advisor is essential. Psychological operations personnel should be augmenting DO personnel. The purpose of psychological operations is to help the commander change behavior. The after-action report from the 800th MP Brigade in Operation *Desert Storm* notes that much of the credit for smooth operations rests with the work of psychological operations personnel.²⁸

Establishing a Combined Joint Interagency Task Force Headquarters

Joint Task Force (JTF) 134 was established after the Abu Ghraib scandal. Its responsibility was the proper care and custody of the detainees throughout the Iraqi area of operations. Included in the custody of the detainees was the mission command of MP operations, MI operations, and the medical commands that

were responsible for detainee medical care.²⁹ The same type of mission command structure was established in Afghanistan around the same time. In 2009, the commander of U.S. Central Command, General David Petraeus, initiated a comprehensive review of U.S. detention operations in Afghanistan. The resulting 700-page report highlighted both the very poor conditions inside Afghan prisons and the potential for radicalization of detainees, and recommended the establishment of a dedicated detentions command in Afghanistan. Based on that assessment, in July of 2009 General Stanley McChrystal, the commander in Afghanistan, requested approval to establish JTF 435 to centralize all detentions, interrogations, medical care, and rule of law functions in Afghanistan.³⁰

The CCDR, in accordance with joint doctrine, is authorized and should immediately establish a Combined Joint Interagency Task Force (CJITF) or Joint Interagency Task Force (JITF) to conduct mission command for DO. This is the most logical conclusion that should be drawn for future operations in which large numbers of detainees are expected. These headquarters need to include staff judge advocates, public affairs personnel, and MP planners. Each day, senior American commanders wake up with the best of intentions. Unfortunately, many of the errors that have occurred in DO have involved the leadership responsible for DO. These failures include ambiguity in the chain of command, poor leadership, a lack of discipline and training, and vague rules of engagement.³¹ Thus, it is important to have a general officer/flag officer (GO/FO) as the commander and deputy commander of this task force. The immediate appointment of a GO/FO will allow the commander to conduct mission analysis and mission command with a functional staff and plan for DO appropriately.

The commander and deputy commander will have an obligation to interact with the International Committee of the Red Cross (ICRC), international media, and key host-nation government officials. Lastly, the CJITF/

JITF commander will be responsible for the disposition of those detainees who are held in the custody of the U.S. military. Planners familiar with the Powell Doctrine should be familiar with the premise that requires there be a plausible exit strategy to avoid endless entanglement. In DO, this translates into a plan to turn over detainees at the conclusion of hostilities. In the Korean War, the repatriation of prisoners became the primary disputed issue during armistice negotiations. This sticking point in the negotiations prolonged the war by a year and a half and resulted in many more casualties.³²

At the conclusion of *Desert Storm*, the 800th MP Brigade and its advisory teams were involved in the transfer of Iraqi EPWs to the Saudi Arabian ministry of defense. Initially, senior members of the brigade were not invited to meet with the Saudi officials, which caused problems because those who did the initial planning had little knowledge of the Geneva Conventions; requirements for processing, transfer, and support of EPWs; or Saudi camp capacities. Many of the Iraqi prisoners did not want to go back to Iraq, resulting in approximately 13,418 prisoners wanting to remain in Saudi custody.³³

In Afghanistan, U.S. forces were up against a mandated timeline in which their authority to hold detainees would expire on December 31, 2014. There was a lack of clear guidance as to what to do with the remaining detainees, and at the tactical level it proved problematic. Issues of this nature must be worked out well in advance.

Lastly, current laws are outdated and have not been reevaluated to consider that we are not always going to be involved in conflicts with nation-states. Both U.S. statutes and international law must be revamped to reflect the fact that the world has changed and nations may be in conflict with terrorist organizations, transnational criminal organizations, and lone terrorist cells (or individual terrorists), all of which make DO even more complex. These individuals may come from a failed or fragile state without an effective government or laws. There may be no functioning government or government

willing to take them back. This is now a problem in the Middle East with the defeat of the so-called Islamic State in Syria.

Once detained, what if any training or reentry programs should be considered for detainees upon repatriation? How will that work with the international community and the host nation to ensure released detainees are not a continued threat on the battlefield and to the national security of the United States and its allies?

Strategic Communications and Public Affairs Considerations

According to the Geneva Conventions, the detaining power is responsible for the treatment provided. Within that responsibility, it is specified that the detaining nation will provide safe, humane, and legal custody of all detainees in their custody. Detainees must be fed, sheltered, and provided medical care. Most U.S. commanders are committed to upholding policies and international law that support human rights based on our values and because of the order/safety that humane treatment brings to a facility or camp. To ensure these mandates are met, those responsible for the care, custody, and control of detainees can expect to be visited by the ICRC. The mission statement of the ICRC calls for an impartial, neutral, and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide detainees with assistance. Detainees are protected by the Geneva Conventions, which also give the ICRC the right to visit them. The main ICRC concern is that detainees are treated according to international humanitarian law.

Camps and the process/methodology of DO will be under scrutiny from external sources such as the ICRC and potentially allied nations that entrust the United States to conduct theater-level DO. A commander can also expect the national and international media to be very interested in reporting on DO. Regardless of how well a nation's military is trained and resourced, there are going to be difficult times, and the media will



Iraqi soldiers from 3rd Brigade, 5th Iraqi army, question apprehended insurgents at detainee collection point during Operation Peninsula, in Wasit Province, Iraq, May 20, 2005 (U.S. Army/Arthur Hamilton)

be there to exploit and report on the errors of this operation, thus exposing potential incompetence or detainee mistreatment to the international community. Detainees will ensure there are mistakes and errors made by the guard force as a means of continued resistance. This mission will also draw the interest of various entities within the Department of Defense, and the DO camp commander will be inspected by various U.S. military entities to ensure compliance with appropriate rules and regulations.

If senior leaders are still concerned about “blowing things up,” they are at the tactical level of war and need to get out of that mindset. GO/FOs responsible for the strategic/operational plans need to conceptualize the battlefield and how the campaign will progress and plan both strategically and operationally. In both the Korean War and the war on terror (including Iraq, Afghanistan, and Guantánamo

Bay), the planning, if done at all, was not staffed or tested. Senior leaders must consider the friction of war as described by Carl von Clausewitz. Friction is caused mainly by the dangers of war, its demanding physical efforts, and the presence of unclear information—that is, the “fog of war.” Additionally, one must always consider that everything in war is simple; however, even the simplest thing can be difficult. Lastly, especially regarding DO, remember the old adage that the enemy will always get a vote and “Murphy” will always be present. The failure to consider and plan for DO will create media sensations, public discourse, and continued legal battles over detention procedures that have the potential to jeopardize the mission.

Conclusion

There may be great reasons why planners in previous engagements did not

devote the time and manpower to DO planning. Some may argue that it was not a major concern, while others might suggest it just was not what warfighters do. Combat operations are hard, and American Forces are subject to death. There is no one that can disagree with that reasoning. However, the United States can ill-afford to win certain phases while losing others, particularly one that has captured the attention of the international media and various human rights groups. The inability to properly plan and resource DO has resulted in unnecessary injury and death for American and allied warfighters. It has also resulted in increased scrutiny and embarrassment for the U.S. military, in particular senior leadership. Elected officials have also come under inquiry based on this aspect of the plan.

Based on the foregoing discussion, no one can dispute the fact that tactical-level

DO can have strategic implications in the international arena. Based on that logic, would it not make more sense to ensure the plan is intact while we are at peace, rather than try to create a plan, or improve on an unstaffed plan, during actual conflict? If the latter choice is made, then truly more Americans will be subjected to the brutalities of combat based on a changing or untested plan. This article should serve as a notice to GO/FO and planners on CCMD staffs as to what they can expect in this difficult but important mission. The U.S. military can no longer muddle its way into this aspect of the plan and then hope for success. Historically, that has proved ineffective and costly. JFQ

Notes

¹ Joint Publication (JP) 3-63, *Detainee Operations* (Washington, DC: The Joint Staff, November 13, 2014).

² Allan R. Millet, *The War for Korea, 1950–1951: They Came from the North* (Lawrence: University Press of Kansas, 2010).

³ T.R. Fehrenbach, *This Kind of War: The Classic Korean War History* (Washington, DC: Potomac Books, Inc., 2000).

⁴ Monica Kim, “Humanity Interrogated: Empire, Nation, and the Political Subject in U.S. and UN-Controlled POW Camps of the Korean War, 1942–1960” (Ph.D. diss., University of Michigan, 2011).

⁵ Lindesay Parrot, “Koje Riots Linked to Truce Leaders,” *New York Times*, January 29, 1953.

⁶ Richard Peters and Xiaobing Li, *Voices from the Korean War: Personal Stories of American, Korean, and Chinese Soldiers* (Louisville: University Press of Kentucky, 2005).

⁷ Fehrenbach, *This Kind of War*.

⁸ Walter G. Hermes, *Truce Tent and Fighting Front*, vol. 2 (Washington, DC: Office of the Chief of Military History, Department of the Army, 1970).

⁹ The entire episode can be found in Harold J. Vetter, *Mutiny on Koje Island* (North Clarendon, VT: C.E. Tuttle Company, 1965), a must-read book for any officer involved in detainee operations, including general and flag officers.

¹⁰ George Forty, *At War in Korea* (New York: Random House, 1985).

¹¹ Vetter, *Mutiny on Koje Island*.

¹² Ibid.

¹³ Ibid.

¹⁴ James R. Schlesinger, chairman, *Final Report of the Independent Panel to Review DOD Detention Operations* (Washington, DC: Department of Defense, 2004).

¹⁵ Ibid.

¹⁶ Richard W. Stewart, *The United States Army in Afghanistan: Operation Enduring Freedom, October 2001–March 2002* (Washington, DC: U.S. Army Center of Military History, n.d.).

¹⁷ See Adam Roberts, “The Prisoner Question: If the U.S. Has Acted Lawfully, What’s the Furor About?” *Washington Post*, February 3, 2002.

¹⁸ Eric Schmitt, “Career of General in Charge During Abu Ghraib May End,” *New York Times*, December 5, 2006.

¹⁹ Samuel L. Brenner, “I Am a Bit Sickened?: Examining Archetypes of Congressional War Crimes Oversight after My Lai and Abu Ghraib,” *Military Law Review* 205 (Fall 2010), 1.

²⁰ Cheryl Benard et al., *The Battle Behind the Wire: U.S. Prisoner and Detainee Operations from World War II to Iraq* (Santa Monica, CA: RAND, 2011).

²¹ Niall Ferguson, “Prisoner Taking and Prisoner Killing in the Age of Total War: Towards a Political Economy of Military Defeat,” *War in History* 11, no. 2 (April 2004), 148–192.

²² Ibid.

²³ Arnold Kramer, “Japanese Prisoners of War in America,” *Pacific Historical Review* 52, no. 1 (February 1983), 67–91.

²⁴ John R. Brinkerhoff, Ted Silva, and John Seitz, *United States Army Reserve in Operation Desert Storm. Enemy Prisoner of War Operations: The 800th Military Police Brigade* (Alexandria, VA: Institute for Defense Analyses, 1992).

²⁵ James B. Brown, Erik W. Goepner, and James M. Clark, “Detention Operations, Behavior Modification, and Counterinsurgency,” *Military Review*, May–June 2009.

²⁶ Field Manual 3-63, *Detainee Operations* (Washington, DC: Headquarters Department of the Army, 2014).

²⁷ Anne Speckhard and Ardian Shajkovci, “Prison: Militant Jihadist Recruiting Grounds or Refuge for Rehabilitation?” *Homeland Security Today*, December 11, 2018.

²⁸ Brinkerhoff, Silva, and Seitz, *United States Army Reserve in Operation Desert Storm*.

²⁹ Benard et al., *The Battle Behind the Wire*.

³⁰ Combined Joint Interagency Task Force 435, After Action Report, November 2015.

³¹ Paul T. Bartone, *Lessons of Abu Ghraib: Understanding and Preventing Prisoner Abuse in Military Operations*, Defense Horizons 64 (Washington, DC: NDU Press, 2008).

³² William Roskey, *Koje Island: The 1952 Korean Hostage Crisis*, The Land Warfare Papers, No. 19 (Arlington, VA: Association of the United States Army, September 1994).

³³ Brinkerhoff, Silva, and Seitz, *United States Army Reserve in Operation Desert Storm*.

New from NDU Press

Center for the Study of Chinese Military Affairs

Strategic Forum 303

The PLA Beyond Asia: China's Growing Military Presence in the Red Sea Region

By Joel Wuthnow



China has gradually expanded its military footprint in the Red Sea region, an area of critical importance

for global maritime commerce and energy production. Key aspects include a People’s Liberation Army role in United Nations peacekeeping, anti-piracy patrols, and a new base in Djibouti. China’s military presence—its largest outside the Indo-Pacific—supports Beijing’s diplomatic relations in the region, contributes to China’s maritime security interests, and provides useful lessons in building an expeditionary capability. U.S. officials need to address operational safety and counterintelligence issues and determine whether China’s presence—which also includes military diplomacy and arms sales—is eroding traditional U.S. advantages as a security partner. Opportunities for military cooperation should be explored in areas where U.S. and Chinese interests align, such as disaster management and maritime safety.



Visit the NDU Press Web site for more information on publications at ndupress.ndu.edu

Screening Obscuration Module attached to Utility Task Vehicle activates autonomously during Robotic Complex Breach Concept on Yakima Training Center, Yakima, Washington, April 26, 2019 (U.S. Marine Corps/Nathaniel Q. Hamilton)



Transforming DOD for Agile Multidomain Command and Control

By Douglas O. Creviston

Advances in artificial intelligence (AI) and autonomous systems offer enhanced military capabilities to those nations that adopt and operationalize these technologies. Much like the airplane or nuclear

weapons, these technologies are so significant that the Department of Defense (DOD) should expect to transform in order to fully realize their benefits. Without data, neither human nor artificial intelligence has a basis for

effective decisionmaking. While human intelligence is capable of operating in a sparse data environment, many AI applications require big data sets to come into existence and continuous data flows to effectively operate. Unlike the airplane and nuclear weapons, AI and autonomy will be best operationalized not by a dedicated Service or force structure devoted to their employment, but by their incorporation into the existing forces in all domains. How might DOD need to change policy, leadership structures, and culture regarding data in order to enable the adoption and maximum benefit of AI and autonomous system technologies?

From the academic and business communities, *data science* is defined as a “multidisciplinary field that concerns technologies, processes, and systems to extract knowledge and insight from data and to support reasoning and decisionmaking under various kinds

Colonel Douglas O. Creviston, USAF, is Director of the Comparative Technology Office in the Office of the Under Secretary of Defense for Research and Engineering.

of uncertainty.”¹ The field of data science may be divided into two primary activities: managing the data and using (analyzing) the data. Many of the activities of data science use AI and in turn support the development and operation of autonomous systems.

Advances in AI, autonomous systems, and big data analytics are especially relevant to emerging concepts of multidomain battle and associated multidomain command and control (MDC2). Existing C2 systems and concepts should be reconsidered in light of the transformative potential of AI and autonomy. Such a reevaluation should start with proven C2 theory, modify existing C2 doctrine if needed, and redesign C2 concepts and systems in order to gain additional capability.

While the development of data science technologies is important and necessary, it is not sufficient. This article focuses on insights from the academic and business data science communities concerning the process and system changes necessary to transform DOD to adopt AI and autonomy to MDC2. The recently released DOD Digital Modernization Strategy contains objectives to modernize C2 infrastructure and improve allied interoperability.² The academic field of data science combines with the theory of agile C2 to provide recommendations to enable agile, integrated MDC2 through the adoption of AI and autonomy. These recommendations suggest policy and cultural changes to transform DOD for cognitive, algorithmic warfare.

Agile C2 Theory Applied to MDC2

According to joint doctrine, “Command is the most important role undertaken by a JFC [joint force commander]. C2 is the means by which a JFC synchronizes and/or integrates joint force activities. C2 ties together all the operational functions and tasks and applies to all levels of war and echelons of command.”³ The function (or action) of command and control is separate from the C2 support systems and structures that enable it:

*A C2 support system, which includes interoperable supporting communications systems, is the JFC’s principal tool used to collect, transport, process, share, and protect data and information. To facilitate the execution and processes of C2, military communications systems must furnish rapid, reliable, and secure information throughout the chain of command.*⁴

Agile C2 theory helps explain the linkage between the function of C2 and the tool of the C2 support system by defining three dimensions that can characterize any approach to fulfilling the C2 function:

- how decision rights are allocated
- how entities interact with one another (interactions)
- how information is distributed (linkages).⁵

The JFC should define these dimensions depending on the objectives, threat, and environment. MDC2 fundamentally asserts that future conflicts will require C2 agility—the ability to alter decision rights, interaction patterns, and information distribution to effectively integrate and synchronize operations across multiple domains—in order to prevail.

Design for Agility in MDC2

C2 support systems should be designed to offer the JFC the maximum design space along the three dimensions of agile C2 theory: decision rights, interactions, and linkages.⁶ Design space is here used as the range of possible options for each of the three dimensions. Current C2 support systems constrain the C2 design space; decision rights might not be allocated to the desired subordinate commander because interactions and linkages are either not possible or do not meet requirements for rapidity, reliability, or security. For example, a JFC may want to allocate the decision rights for air defense of a certain sector to a particular field commander, but the interactions and linkages may not support the flow of requisite data to the desired level of field command. Data science can help through infrastructure designs and

analytical tools that enable real-time governance of interactions and linkages as determined by the JFC’s allocation of decision rights. In addition, data science should be applied to each tenet and subdomain of C2—for example, by using recommender systems (market basket analysis or others) to curate information flows to decisionmakers and operators at every level and in every domain.

David Perkins and James Holmes have described the concept of multidomain battle and the reason it is needed. Historically, each Service has developed federated solutions (weapons, concepts, capabilities) in that Service’s operational domain. These were then “synchronized” in a tailored joint response to a specific problem. The time and effort required to synchronize will not support future mission success, and currently possible mash-ups of federated capabilities will still be vulnerable to fracture along Service boundaries.⁷ Future C2 systems are already in development, including the Air Force’s in-house reboot of the canceled Falconer 10.2 upgrade, as well as the Army’s restructuring of the Warfighter Information Network—Tactical program and modernization of the Nuclear Command, Control, and Communication system. As these systems are developed, key performance attributes should include integration and agility in addition to basic network requirements such as cyber security, resilience, and so forth.

Future C2 systems must be integrated and agile. Joint Publication 1, *Doctrine for the Armed Forces of the United States*, posits, “The simplest and most streamlined chain of command can be thwarted by an absence of interoperability among the components’ forces and systems.”⁸ Interoperability is no longer enough, as Perkins and Holmes imply when they state, “We must shift from a model of interdependence to one of integration.”⁹ Such an integrated architecture would support the improvement they cite as most important: sensor-to-shooter webs. Investment should be made in automated data management tools (for example, a unit assigned a mission will automatically



Seaman uses handheld tablet to request resupply during Office of Naval Research demonstration of Autonomous Aerial Cargo/Utility System, giving capability to helicopters for unmanned flight, Quantico, Virginia, February 25, 2014 (U.S. Navy/John F. Williams)

be routed intelligence feeds related to that mission and operational feeds related to relevant missions in every domain).

As an example, near-future integrated air and missile defense (IAMD) against peer competitors in an anti-access/area-denial environment will rely on improved integration and information-sharing between sensors (often multirole) and shooters (often multiuse).¹⁰ Rear Admiral Archer Macy, USN (Ret.), now a member of the Missile Defense Project at the Center for Strategic and International Studies, identified employment and C2 doctrine as one of the biggest challenges facing IAMD in the transition to a distributed defense approach. When two military Services are shooting using sensor data from four military Services and national agencies, the challenge of allocating

information and authority to all the right nodes becomes immense.¹¹ C2 agility is required to meet this challenge.

Agility is here defined as adaptability (ability to change with the situation) with the added qualities of ease and timeliness of adaptation.¹² Agility is achieved in different ways depending on the attribute that must be changed. Agility in infrastructure may mean procuring multiple pathways for data and designing automated or low-work methods for switching between them. Agility in analysis may come through data management able to provide comprehensive data in an environment populated with open-source or licensed tools and a workforce trained to use them.

The need for tactical and C2 networks to be integrated runs counter to the organizational and funding approaches to

developing those networks. The Services develop networks to meet their own needs, on their own acquisition schedules, with interoperability requirements imposed from the Joint Staff. This lack of synchronization in acquisition and development results in integration challenges and reduced C2 capability.¹³

Current C2 systems constrain the JFC's ability to allocate decision rights by limiting the linkages that are possible or permissible and what information can flow over the set of possible linkages. They are not integrated or agile enough to support MDC2. These systems have grown out of organizational, cultural, and security decisions that shaped previous system design and operational use. At the turn of the century, DOD leaders sought to apply network technology and concepts to remake the Armed Forces.

What can we learn from the 2003 DOD Net-Centric Data Strategy and resulting attempts to remake C2 networks and tactical network systems?

Lessons from the DOD Net-Centric Data Strategy

Network-centric warfare was introduced by Vice Admiral Arthur Cebrowski, Dave Alberts, and John Garstka in the late 1990s. It sought to maximize combat power through the effective linking (networking) of geographically dispersed forces, resulting in shared battlespace awareness that enables self-synchronization and synergistic action.¹⁴ The information technology implementation of network-centric warfare inspired the 2003 strategy.¹⁵

The strategy sought to remake department data flow from prescribed point-to-point transfers across highly controlled interfaces to flexible many-to-many interchanges within a global enterprise data environment. It supported the DOD chief information officer (CIO) goal to “populate the network with all data (intelligence, non-intelligence, raw, and processed)” — a wide goal that has not been realized to this day with separate networks for intelligence and non-intelligence data. Furthermore, the strategy proposed to change the paradigm to “post before processing” rather than waiting to post after completion of a “processing, exploitation, dissemination” cycle. Other features still relevant yet unfulfilled include an enterprise metadata registry, a data catalogue, and establishment of interface standards to facilitate flexible interfaces unforeseen during development of an information system. The strategy defined data attributes essential to meeting performance goals—data was to become visible, accessible, institutionalized, understandable, trusted, interoperable, and responsive to user needs.¹⁶ The goals of the strategy are echoed in recent DOD and Service guidance; they are still relevant and desirable but have proved elusive. The strategy accurately understood important shifts in the global information environment and proposed sweeping

changes to adapt. What factors limited the realization of the strategy?

Priscilla Guthrie, a key instigator of the strategy and DOD deputy CIO at the time, identified communication as a central shortcoming. In 2003, data science advocates failed to clearly communicate the business and operational case for implementing the data strategy. The theory of information, semantic technology, technical capabilities of information technology, and computer science jargon was meaningless to most DOD senior leaders, military and civilian alike.¹⁷ Private-sector examples of effective data science existed, but they were nascent. In this respect, the situation is somewhat better in 2020 as private-sector success stories abound in the business results of data-centric companies such as Google, Amazon, Microsoft, and Facebook, and popular interest in AI/machine learning is captured by public demonstrations from AlphaGo to autonomous package delivery.

Leadership support in 2003 was neither sustained nor strong due to leadership transitions and lack of understanding. According to Guthrie, DOD did not have the human resources to effectively acquire, implement, and operate a modern data infrastructure and failed to develop viable contract vehicles to remedy the shortfall.¹⁸ Implementation of the data strategy also stalled because of the failure to field a viable metadata registry and data catalog, necessary to any effective execution of data science. DOD failed to enact a viable resourcing plan to support the strategy. As a cross-cutting, foundational capability, data infrastructure needed a single champion to advocate for investment and a stable, multiyear funding stream.

The 2003 strategy was a forward-thinking document that failed to achieve the desired result. The primary reasons for that failure were lack of leadership support due to lack of understanding; failure to make necessary cultural, organizational, and policy changes; inadequate in-house human resources and failure to acquire adequate external human resources; and inadequate financial resources due to a flawed funding strategy.

DOD problems with implementation of the strategy have cost billions of dollars, years of effort, and lost combat effectiveness. As a foundational step toward effective MDC2, senior leaders should address the key factors contributing to that failure. The strategy was not a perfect document, and network-centric warfare was not a perfect concept, but those imperfections will be an inherent part of current and future strategy and concept development. The new DOD Digital Modernization Strategy outlines a strategic plan for resource investment in fiscal years 2019 to 2023 and continues with many themes evolved from network-centric warfare and the 2003 data strategy, but with greater specificity of mission objectives and a plan for incorporating cutting-edge information technologies. To effectively execute digital modernization of DOD, senior leaders will need to resolve important cost-benefit tradeoff decisions that were and will be inherent to any major policy, organizational, and resourcing shifts. Data science as an academic discipline offers insights that can guide leadership decisions. Individual applications will pose unique challenges and require unique solutions, but data science provides the theoretical principles and disciplined process by which the department can adopt AI and autonomy to turn data into military capability.

Data Science Defined

To reiterate, data science is “a multidisciplinary field that concerns technologies, processes, and systems to extract knowledge and insight from data and to support reasoning and decisionmaking under various kinds of uncertainty.”¹⁹ This field may be divided into two primary activities: managing the data and using (analyzing) the data. Data management encompasses the collection, storage, cleaning, engineering, and monitoring activities required to give data the desired attributes that make it useful.²⁰ To be useful, data must be visible, accessible, understandable, trustworthy, and interoperable.²¹ Data is used through data analytics in activities also known as business intelligence



Fourth-year Ph.D. student Mark Veleznitsky, University of California, Berkeley, discusses his research during Naval Postgraduate School Operations Research Department's second annual Day of Data, Decisions, and Defense, Monterey, California, August 27, 2018 (U.S. Navy/Javier Chagoya)

and big data analytics and encompasses descriptive, predictive, and prescriptive analytics. This article includes within the definition of *data science* the management and organizational processes and systems necessary to enable the application of data management and analytics technologies—sometimes also referred to as the “digital transformation” or “digital modernization” of an organization.

Data Science: Forcing, Enabling, and Enabled Technologies

Forcing technologies push data science by creating data problems requiring data science to solve. The proliferation of sensors, storage and computing power, and network connectivity has resulted in substantial growth in the volume and variety of data that must be managed. Practicing data analytics creates new data about data. The

Internet of Things promises penetration of this sense/store/compute/network structure into previously data-sparse environments. The resulting flood of data renders legacy human-centered approaches to analysis and decisionmaking ineffective; the dominant challenge has changed from one of sensing and collecting data to one of processing, cataloguing, searching, and verifying useful data. These forcing technologies have combined to increase the volume, velocity, and variety of relevant data beyond the capability of legacy infrastructure and analytic capabilities.

Data science often uses statistical methods that are old concepts applied in new ways. The key enabling technologies have been increased computing processing power and memory at decreased cost, increased data generation throughout the environment, and massive parallel data architectures that enable efficient storage

and processing of data at the point of storage (virtualization). These advances combine to make statistical concepts that were prohibitively expensive in either time or money practical for a wide range of users.

Data science enables one to sense reality in many ways and then perform computationally expensive but conceptually simple algorithms to allow an intelligence (human or artificial) to understand reality more fully and accurately. Technologies enabled by data science include descriptive, predictive, and prescriptive analytics, AI, and autonomy. Major technological trends have dramatically changed the volume, variety, and velocity of data available for MDC2 as well as the operational benefit that may be gained from that data. Extracting that operational benefit requires overcoming the obstacles that derailed full implementation of the 2003 data strategy.

Recommendations for Agile MDC2

Proposals to enable effective MDC2 are derived from historical examples and civilian literature on digital transformation of complex business operations. DOD has repeatedly fallen short of strategic goals relative to data and network-centric warfare, in part due to excessive focus on the technology and acquisition thereof. The Defense Innovation Board captured the link between the first three recommendation areas when it stated, “Since many of the Department’s challenges with data are cultural (that is, DOD organizations are not used to collecting or sharing data), the Secretary’s role in this endeavor is critical, particularly because new policy and legal frameworks will be necessary to change the status quo.”²² None of these recommendations are binary; each requires leadership judgment to select an approach that balances present and future risk, funding limitations, statutory authority, and so forth. Leandro Dallemule and Thomas Davenport have discussed how leaders can define the overall posture of an organization relative to “offensive” and “defensive” uses of data and show how different governance, organizational structures, and resourcing approaches are best suited to each set of uses.²³ The foundational concept behind these recommendations, born out of a reading of the civilian literature on data science and digital modernization, is that senior leaders should take a holistic approach to transform DOD for the application of AI and autonomous technologies, for both MDC2 and other mission areas. The 2019 DOD Digital Modernization Strategy outlines ambitious and much-needed goals and objectives to transform DOD. What are the difficult policy, cultural, and organizational tradeoffs leaders should expect to make, and what resources are available to support those decisions?

Recommendation One: Senior Leaders Should Implement Data Science as a Multidisciplinary Field to Guide Transformation of Policy, Organization, and Resourcing Decisions. Leaders must

make foundational decisions to achieve coherence among data management, data analytics, and the overall strategy and trajectory of DOD as AI and autonomous technologies are acquired and fielded. At the department level, leaders can learn from civilian management experiences of transforming companies and institutions to inform difficult tradeoff decisions. Transitioning C2 from an industrial-age approach to an AI-enhanced one will require leaders to initiate and sustain the transformation with a changing threat environment and emerging multidomain battle concepts. This includes the development and acquisition of C2 support systems that maximize the design space available to JFCs and that are delivered integrated and agile to support joint and coalition operations. The acquisition of such systems may require a different allocation of acquisition resources and/or oversight in order to synchronize disparate efforts. Instead of viewing data science (or AI or autonomy) as a tool to be bought, commanders should recognize data science as a discipline practiced to enable better decisionmaking.²⁴ This recognition should include experimentation with different allocations of decision rights, interactions, and linkages to explore the effects of different concepts in contested peer conflict. Without senior leader support to initiate and persistently support the application of data science, the existing conflicts among policy, organizational priorities, and parochial interests will continue to forestall system design, acquisition, experimentation, and operational execution of MDC2.

Recommendation Two: DOD Senior Leaders Should Promote Cultural Values of Data Collection, Evidence, and Cooperation (Data-Sharing). DOD does not appropriately value data. Data is valued relative to the primary purpose for which it is collected. One tenet of data science is that data is inherently valuable and may be used to extract value in many ways beyond the purposes for which it was originally collected.

The dominant DOD cultural value regarding data is one of protection within organizations on the smallest level—except where forced by leader action or

policy. Leaders from the top down should recognize the value of sharing data and require open analysis, including the sharing of underlying data as well as analytic methodologies to support evidence-based decisions. To support and encourage a culture of data-sharing, policy should be shaped to promote the needed analysis to generate decision-quality evidence with the minimum interference required for governance and security needs.

Recommendation Three: Leadership Should Issue Clear, Consistent Policy

Promoting Data Availability at Acceptable Risk. Senior leader calls for innovation and rapid acquisition are sometimes undercut by data governance policy (or lack thereof) that allows compartmentalization to persist. This is a problem that subordinate units are unable to solve in a timely manner. Governance policy should cover data ownership, access, use, protection, and disposition. In addition, governance could extend to validation of data sets as authoritative or of analysis as technically sound. Data sets will have unique risk/reward characteristics based on their content and potential uses. As with any policy, data governance policy should be clear and consistent to define the boundaries of acceptable action and promote freedom within those boundaries. In addition to clarity and consistency, policy should be evaluated over time to determine effectiveness. This evaluation should be an explicit part of joint exercises and operations; if data-sharing policy does not support mission success, the policy must be changed.

Recommendation Four: Develop a Methodology for Assessing the Value of Sharing Data. For classified and compartmented data, “need to know” is a policy, not only a cultural mindset. Security policy is authoritative, communicating leadership decisions about the acceptable risk/reward ratio for data access. To support those decisions, estimates should be developed for the damage to national security due both to information escape and ill-informed decisions or to operational failures because of incomplete information. A well-structured data science effort should consider



Army UH-60 "Blackhawk" flies in formation over Yamaguchi Bay, Japan, during premier U.S. Army and Japan Ground Self-Defense Force bilateral field training exercise Orient Shield 2019, September 9, 2019 (U.S. Army/Jacob Kohrs)

a means of quantifying these two estimates (loss due to sharing and loss due to not sharing) into a decision support system for information-sharing decisions. Such decisions may include lowering the classification level of information over time, sharing information with certain allies or coalition partners, or removing a compartmentation or special access program caveat to allow wider awareness and incorporation of an operational capability. Leadership statements about the importance of concepts, such as sensor-shooter networks in multidomain battle and technologies such as AI, to victory in future conflict must be converted into security policy changes that permit adoption of those concepts and technologies with appropriate, accepted risk to information flows. There are technologies to improve the risk/reward ratio of information-sharing decisions, but these do not fully resolve the inherent reduction

in information security that comes with increased access to the information.

Recommendation Five: Vest Security Decision Authority Where Risk and Reward Meet, at an Appropriate Level Within the Chain of Command.

Commanders at every level should be given clear, expanded "right to share" authority over information and information systems. In addition to providing a decision support system for information-sharing decisions, policy should be changed to vest those decisions in the chain of command. Existing policy puts operational effectiveness at risk by endowing security professionals outside and disconnected from the chain of command with final authority for information-sharing decisions, at both the infrastructure level (network infrastructure authority to connect/authority to operate) and the operational level (the ability to disclose a particular element

of operational or intelligence data to a subordinate decisionmaker or operator). Furthermore, some intelligence and acquisition agencies restrict the range of possible information linkages available to the operational commander through compartmentalization or special access programs. The chain of command should be given a right to share authority over all information the commander has access to for all members, U.S. and coalition, under his or her command. This right to share will likely require limits to protect strategic interests and/or prevent the present chain of command from reaping current rewards at the cost of increased future risk.

As an example, a joint task force commander may be given authority to share classified information not specifically cleared for foreign disclosure with a coalition partner who possesses a comparable security clearance. As an additional

example, a combatant commander may be given authority to grant access to special access programs to members of his or her command deemed necessary, but subject to the limitation that those members have a clearance at the overall classification level. There are existing processes for both of the above examples that reflect a certain static risk/reward tradeoff decision, but those processes and the underlying tradeoff decision should be reevaluated in light of the accelerated pace of warfare, knowledge, and information flows required for successful implementation of AI and autonomous technologies.

Recommendation Six: Contract for Partnership to Build Government Capability in C2 Support Systems. Agile C2 support systems likely cannot be acquired as traditional vendor-supplied systems with proprietary architecture, both because contracting (and associated legal) timelines are too long and because DOD human resources with intimate understanding of the C2 support system are required. DOD has inadequate capability and capacity of human resources to implement data science in command and control, so contractor support will be required for some time. Contractor personnel could provide support services with appropriate contract vehicles that avoid proprietary solutions, produce data and tools that are government property, and surge human resources in areas the government is lacking. The Air Force approach to developing C2 applications in-house seeks to deliver both needed C2 capabilities now and the capacity for agile development of future capabilities. Active-duty Air Force programmers are teamed with those of Pivotal Labs to produce software that is wholly government-owned and may be iteratively developed as requirements change.²⁵ DOD should recognize the need for in-house capability to adapt C2 support systems in the combat zone and invest in equipment and training to develop that capability.

Future warfare will incorporate two broad trends: multidomain battle and AI/autonomy. Both trends demand a higher level of interoperability,

even integration, of data networks to be successful. Across the range from competition to conflict, joint force commanders will need maximum design space in the three agile C2 dimensions of decision authorities, interactions, and linkages to develop effective multidomain C2 approaches. DOD has pursued transformation to a network-centric force before, but with limited success. Learning from the implementation of the 2003 data strategy, senior leaders should apply data science theory from the civilian world to evaluate what deep cultural, organizational, and policy changes may be necessary to adopt the transformative technologies of AI and autonomy. Future multidomain battles will be complex, and that complexity cannot be eliminated with technology. Developing agile and integrated C2 support systems may enable future JFCs to prevail over the enemy despite the complexity. *JFQ*

Notes

¹ National Academies of Sciences, Engineering, and Medicine, *Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions* (Washington DC: National Academies Press, 2017), 1–2.

² *DOD Digital Modernization Strategy* (Washington, DC: Department of Defense, June 5, 2019), available at <<https://media.defense.gov/2019/jul/12/2002156622/-1/-1/dod-digital-modernization-strategy-2019.pdf>>.

³ Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, incorporating change 1, July 12, 2017), xxiii.

⁴ *Ibid.*, xxiv.

⁵ David S. Alberts et al., *C2 by Design: Putting Command and Control Agility Theory into Practice*, version 2.0, NS D-5614 (Alexandria, VA: IDA, 2015), 14.

⁶ David S. Alberts, Reiner K. Huber, and James Moffat, *NATO NEC C2 Maturity Model* (Washington, DC: DOD Command and Control Research Program [CCRP], 2010), xvii.

⁷ David G. Perkins and James M. Holmes, “Multidomain Battle: Converging Concepts Toward a Joint Solution,” *Joint Force Quarterly* 88 (1st Quarter 2018), 54–57.

⁸ JP 1, V-19.

⁹ Perkins and Holmes, “Multidomain Battle,” 54–57.

¹⁰ Thomas Karako and Wes Rumbaugh, *Distributed Defense: New Operational Concepts for Integrated Air and Missile Defense* (Washington, DC: Center for Strategic and International Studies [CSIS], January 2018), available at <<http://missilethreat.csis.org/wp-content/uploads/2018/01/Distributed-Defense.pdf>>.

¹¹ Remarks from January 25, 2018, release of the *Distributed Defense* report at CSIS.

¹² Alberts et al., *C2 by Design*, 6.

¹³ Brian K. Bass et al., “Overcoming Joint Interoperability Challenges,” *Joint Force Quarterly* 74 (3rd Quarter 2014), 136–140. See figure 2.

¹⁴ David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare* (Washington, DC: CCRP, 1999), 88.

¹⁵ *DOD Net-Centric Data Strategy*, memorandum, May 9, 2003, available at <<http://dodcio.defense.gov/Portals/0/Documents/DIEA/Net-Centric-Data-Strategy-2003-05-092.pdf>>.

¹⁶ *Ibid.*

¹⁷ Priscilla Guthrie, interview by author, December 7, 2017.

¹⁸ *Ibid.*

¹⁹ National Academies of Sciences, Engineering, and Medicine, *Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions*, 1–2.

²⁰ *Ibid.*, 2.

²¹ *DOD Net-Centric Data Strategy*. These five attributes were identified in the 2003 DOD Data Strategy and are repeated verbatim in the 2017 Navy Data Strategy and 2016 Army Data Strategy. The Air Force substitutes the phrase *link context* for the term *interoperability* to form the acronym VAULT (visible, accessible, understandable, linked, and trustworthy), but it retains the essential attribute characteristics.

²² Defense Innovation Board, *Practices and Operations—Recommendation 12: Forge New Approach to Data Collection, Sharing, and Analysis*, March 19, 2018, available at <<http://innovation.defense.gov/Recommendations/>>.

²³ Leandro DalleMule and Thomas H. Davenport, “What’s Your Data Strategy?” *Harvard Business Review* (May–June 2017), 112–121. The authors characterize the overall posture of an organization relative to “offensive” and “defensive” uses of data and show how different governance, organizational structures, and resourcing approaches are best suited to each set of uses.

²⁴ Defense Innovation Board, *Practices and Operations*.

²⁵ Mark Wallace, “The U.S. Air Force Learned to Code—and Saved the Pentagon Millions,” *Fast Company*, July 5, 2018, available at <www.fastcompany.com/40588729/the-air-force-learned-to-code-and-saved-the-pentagon-millions>.



Marine with 2nd Battalion, 7th Marines, carries sandbag to strengthen security post during reinforcement of U.S. Embassy Compound in Baghdad, January 4, 2020
(U.S. Marine Corps/Kyle C. Talbot)

Disciplined Lethality

Expanding Competition with Iran in an Age of Nation-State Rivalries

By Scott J. Harr

The United States had formerly enjoyed distinct competitive advantages prosecuting armed conflict in the war on terror around the globe. However, the swift ascension of states such as China, Russia, and Iran in terms of regional and global capabilities to project power, coupled with the exhausting U.S. focus on defeating violent extremist organizations over the better part of two decades, requires a reevaluation of strategy. This shift is

neither new nor unanticipated. As articulated in the 2018 National Defense Strategy (NDS), strategic competition between the world's Great Powers will define the new operational environment moving forward.¹ Rising near-peer competitors are using innovative technology and seizing on ambiguities within the new and emerging battlespace to make strategic gains on the margins of peace that nullify or bypass traditional American strengths.

The NDS has fittingly put a premium on "expanding the competitive space" with adversaries.² While prioritizing lethal force, the NDS also identifies the imperative to leverage all elements of national

power in efforts to "expand" the competition, which implies a preference to keep competition at levels of confrontation at the level beneath open warfare. As one of the four states identified in the NDS and the Middle East's preeminent near-peer adversary of the United States, Iran naturally dominates discussions on emerging security challenges, and senior leaders from the highest echelons of defense policy have prioritized countering Iran's "malign" influence in the region.³

Given the above, the intent of this article is to analyze the nature and prospects of expanding strategic competition with Iran in the Middle East. In order to best understand the nature of strategic

Major Scott J. Harr, USA, is a Company Commander in 5th Special Forces Group (Airborne).



Republic of Korea army soldiers stand resolute at Joint Security Area where South and North Korean soldiers stand face-to-face across Korean Demilitarized Zone, Panmunjom, South Korea, June 19, 2018 (U.S. Army/Richard Colletta)

competition with Iran, it is first necessary to identify some unique aspects of Iran as a near-peer adversary compared to other states. This article first distills the salient factors that impact approaches to strategic competition with Iran. Next, it analyzes the pertinent dynamics governing strategic competition given the prevailing competitive approaches that undergird each country. Finally, based on the preceding analysis and findings, it offers recommendations for strategic actions to guide U.S. competition against Iran and steer approaches to favorable outcomes for U.S. interests. Competitive actions and strategies that are attuned to the unique aspects of Iran as a near-peer adversary and that account for the existing dynamics governing Iran's approach to competition in the Middle East stand a better chance of thwarting Iranian attempts to undermine U.S. power and influence in the space between war and peace. Such actions also represent

the best chance to stabilize the Middle East amid robust Iranian efforts to the contrary.

Gray Zone Competition: A Near-Peer Without Peer

The NDS primarily speaks of national threats emanating from four nations: China, Russia, North Korea, and Iran. All these states currently compete against the United States in what some have termed the gray zone, which, as noted by scholar Van Jackson, generally denotes types of conflict "short of war" or, essentially, "non-war competition" between states.⁴ Near-peer competition in the gray zone is not created equal, and the four states identified in the NDS go about their competition differently and take up decidedly diverse competitive strategies and tactics undermining U.S. interests and sovereignty. Therefore, in order to isolate the character of Iran's competi-

tive strategy with an eye toward recommending effective counterstrategies, it is useful to compare the attributes of how the four states *directly* compete with the United States on the global stage. In defining direct competition, the avenues available for direct engagement, the presence or lack of direct threats emanating from competitor countries, and the level of innovation involved in actions that directly target the United States comprise the lens for this analysis. While other important and significant indirect categories of interaction exist, such as economic relations and the third-party allies and adversaries of the state threats, this analysis focuses on direct actions only. In this way, unique elements of Iran's direct competitive tactics and strategy emerge that ultimately impact the range of feasible and desirable U.S. approaches to engaging in strategic competition with Tehran.

As a starting point for analyzing the direct attributes of near-peer competition from the four states, it is perhaps best to examine what (if any) other elements of national power (besides military action) exist as a venue for engagement. Both Russia and China maintain diplomatic relations with the United States, which instantly expands the possibilities for strategic competition by leveraging diplomacy as a cornerstone element of U.S. power. President Donald Trump has held direct talks with both his Russian and Chinese counterparts during his term.⁵ Such avenues for dialogue make communicating intentions and potentially de-escalating tension profoundly simpler and, by default, augment the range of options available during gray zone conflict. By contrast, limited diplomatic channels exist between the United States, North Korea, and Iran. This characteristic is primarily what distinguishes these states as “rogue” regimes in the NDS. While President Trump has held direct talks with Kim Jong-un and offered to meet with President Hasan Rohani, the lack of official relations and absence of U.S. Embassies in either country promote hostility while straining efforts at communication.⁶

Related to the presence or lack of diplomatic channels between the United States and the four states is the presence or absence of overtly hostile threats of force emanating from these competitors. Both China and Russia have refrained from issuing direct threats of lethal force against the United States despite pointed clashes over issues of sovereignty and economic flashpoints. Indeed, the United States and Russia have gone to great lengths to coordinate and de-conflict their respective actions in the military conflict in Syria to avoid direct confrontation, despite finding themselves on opposite sides of the conflict.⁷ For its part, China and the United States have recently entered a period of détente in a bitter contest of wills regarding international trade and commerce.⁸ These dynamics signify that nations, while fiercely competitive and assertive in fighting for their interests, are reticent to escalate competition to open warfare. As

such, a broader range of options likely exists for the United States to engage in strategic competition options that integrate all elements of national power and imply a supporting role for the military. On the other hand, both North Korea and Iran routinely issue hostile threats of lethal force against the United States while openly flaunting destabilizing military activities such as ballistic missile testing. These bellicose threats, coupled with the lack of diplomatic relations, restrict the elements of national power that can be leveraged in competition while also instantly ushering the military to the forefront of competitive actions to counter the threats.

Finally, the nature of strategic competition between the United States and the four states can be examined in terms of the level of innovation demonstrated in competitive actions. As noted by General Joseph Dunford, modern warfare is changing with the advent of new technologies that near-peer states exploit to make operational gains at the expense of U.S. power.⁹ For instance, Russia has used information operations in creative and plausibly deniable ways to hedge the sovereignty of neighboring states and even allegedly influence democratic elections in the United States.¹⁰ Likewise, North Korea allegedly perpetrated a massive cyber hack of Sony to undermine and delay the release of a commercial film portraying the North Korean regime in a negative light.¹¹ Not to be outdone, China continues to build man-made islands to extend its sovereignty in the South China Sea and use “debt warfare” in Africa to assume control of massive resources and infrastructure on the continent.¹²

All these activities represent innovative competitive actions that exploit technological advances that make attribution difficult or sovereignty issues where policy to guide behavior is currently limited or vague. Iran stands alone in its competitive activities in that it has primarily relied on more traditional tactics to compete in the gray zone. Using a network of proxy forces across the Middle East (notably in Iraq, Lebanon, Syria, and Yemen), Iran successfully projects power

and asserts its foreign policy objectives even without a buildup of conventional military power. Lacking the resources of a Great Power state, Iran nevertheless effectively undermines the security interests of more powerful ones (namely the United States and Israel) by training, arming, and advising capable nonstate actors. As noted by Van Jackson, the use of proxies is a classic tactic employed in gray zone competition and allows the aggressor to offer credible threats of force/retaliation while also obfuscating the actual role of official state apparatus in the support of proxy forces.¹³

Using the analytical framework discussed above, Iran’s direct approach to strategic competition is unique among the four states. In general, it may be stated that the Iranian “brand” of competition restricts the use of all elements of national power, takes an overtly hostile tone, and employs traditional tactics of gray zone warfare. In this sense, Iran represents a “near peer without peer”—that is, competitive responses to Iran will have to address a distinctly Iranian brand of competition. These aspects also ensure that the starting point for strategic competition with Iran appears decidedly more aggressive in nature than other threat states and perhaps diminishes the prospects for expanding competition using softer elements of national power that keep the competition beneath thresholds of warfare.

Hard Truths About Soft Approaches

In addition to seemingly having fewer elements of national power at its disposal to expand competition with Iran, the United States must contend with several constraining dynamics regarding its competition with Iran that impact its strategic approach. Perhaps chief among these dynamics is what might be termed the *competition paradox* that governs the competitive actions of both the United States and Iran in the Middle East. Simply put, the competition paradox theorizes that the freer a country’s civil society, the less free it is to compete in the gray zone. Counterintuitively, a free society’s liberal

values and democratic processes have a constraining effect on the range of competitive actions available in gray zone competition. Societies based on liberal democratic ideals that cherish pluralism, individual liberty, and universal human rights will in general impose limits on their leaders that restrict competitive actions that fall outside liberal societal values. Activities such as arming terrorist groups, conducting cyber attacks on civilian populations, and blatantly violating national sovereignty (all actions taken recently by nondemocratic near-peer competitors) represent unacceptable actions that will likely not be sustainable or viable by the ruling elite in a democratic country with a free civil society.

Naturally, there is some subjectivity and relativism at play here. The United States, as a leading democratic state, has undoubtedly perpetrated questionable or dubious competitive actions to achieve its interests in the past in spite of societal values. However, the important principle that undergirds the competition paradox is that in a free civil society, opposition voices are always present and active, and when thresholds of discontent emerge from the public, democratic mechanisms exist to transition the ruling political power to entities more aligned with the dominant societal values. Conversely, in less free states (like Iran), no mechanisms exist to transition political power, which makes leaders freer to pursue whatever agenda and interests they choose with little restraint and no political constituency to worry about. In Iran, the religious ruling elite have effectively eliminated civil society and concentrated all meaningful political power in unelected bodies and individuals. Their actions and foreign policy agendas are carried out with limited or no opposition and with nothing but the whim of the supreme leader to guide and direct them. This is one reason why Iran can arm paramilitary groups and nonstate proxies in Iraq, Lebanon, Syria, and Yemen that degrade regional stability and engage in terrorist tactics that have been widely condemned by the international community. While the United States enjoys vastly greater individual

and societal freedom than Iran, from the strategic competition standpoint dictated by the competition paradox, Iran is free and the United States is not. Iran, therefore, enjoys a competitive advantage as it presses its foreign policy objectives in the Middle East.

Iran's competitive advantage over the United States is not only derived from the greater degree of freedom it enjoys prosecuting its competitive actions but also stems from diverging and misaligned perspectives on the stakes of the competition itself. For Iran, the stakes of its competition are its very existence, and it therefore perceives its competitive actions as moves made in a "war of necessity," waged for its survival. As noted by Afshon Ostovar in his seminal work *Vanguard of the Imam: Religion, Politics, and the Revolutionary Guard*, since the establishment of the Islamic Republic of Iran in 1979, Iran has viewed Israel as a mortal and existentially threatening enemy. Its foreign policy actions, therefore, endeavor to combat and ultimately defeat Israel. Indeed, Iran has persistently framed its wars and conflicts in terms of creating a "road to Israel" to destroy its nemesis.¹⁴ In this regional power imbalance, as Kenneth Waltz observes, Iran views itself as a lone Persian state surrounded by Arabs and within striking distance of an enemy capable of destroying it.¹⁵ In this context, the stakes could not be higher for Iran, and thus Iran's risk tolerance and resolve to engage in competition are high.

Conversely, for the United States, conflicts in the Middle East represent a war of choice, where only interests—not existence—are at stake. The risk tolerance and resolve for competitive actions in wars of choice are decidedly lower. This misalignment in perspectives between Iran and the United States regarding strategic competition is presumably why Iran is seeking to develop its lethal capabilities, apparently unafraid to escalate the conflict, while the United States is seeking to de-escalate the competition by expanding it to elements of national power that stand a better chance of keeping the competition beneath the level of open warfare.

According to the competition paradox, Iran is both freer to compete in the Middle East and more resolved to do so. Perhaps no one better personified these advantages and their effects on Iran's approach to competition in the Middle East than General Qasem Soleimani, the leader of Iran's special forces (Quds Force) and trusted advisor and instrument of the supreme leader himself. His recent death only highlights his impact within Iran and in the region. As a main architect and executor of Iran's foreign policies in the Middle East, Soleimani was revered in military circles for his success in prosecuting asymmetric military operations that stymied many regional adversaries and blunted the objectives of regional and foreign powers—including the United States—in the Middle East. While Soleimani was undoubtedly a gifted leader who deserved credit for his role helping Iran achieve its foreign policy objectives through asymmetric military approaches, he did not have the mystical prowess or supernatural special warfare abilities frequently alluded to or ascribed to him in contemporary literature. He was, rather, the beneficiary of the dynamics described above: freer to compete and competing with more resolve. Bluntly, Soleimani's gloves were off in competitive approaches designed to preserve and save the Iranian state, while U.S. gloves remain cautiously on as it fights to merely protect its interests abroad. The implications of the U.S.-Iranian competitive dynamics described conveyed decisive advantages to Iran and cast doubt on the viability and prospects of U.S. efforts to expand the competition using reciprocal and/or softer means. Only time will tell if his death will change these dynamics and in what ways.

A Color Evolution: Green-Lighting Red Lines in the Gray Zone

Those who are quick to call for regime change or war with Iran are often pejoratively labeled *Iran hawks* for their aggressive stance. By definition, Iran hawks have given up hope on the prospects for competition in the gray zone. Yet even given the grim prognosis on the current state of competitive play between

the United States and Iran, prospects for effective competition in the gray zone with Iran exist and should be fully explored before giving in to the gravitational pull of yet another large-scale military conflict in the Middle East.

Van Jackson notes that aggressors often make operational gains in the gray zone by taking advantage of either weak or nonexistent red lines from defenders.¹⁶ In this context, *red lines* refer to explicit, clearly communicated, and/or codified in international law boundaries that serve to govern behavior in the gray zone. These lines specify consequences for aggressive actors that cross them. Additionally, the consequences specified for crossing red lines must be credible in order to have the desired deterrent effect. That is, aggressors must believe that defenders will follow through on the punitive actions promised for violations of red lines. Without clear and credible red lines, aggressors can exploit ambiguity and a lack of credibility to make competitive gains. In the current U.S.-Iranian competitive environment, Iran exploits this dynamic to increase its capabilities to wage war in the Middle East at the expense of U.S. credibility. U.S. responses lack either the force or credibility to deter Iranian competitive gains. Sanctions, for example, while crippling the Iranian public and inducing massive hardship in society, are too easily circumvented by the ruling regime and its international allies to stand a real chance at dislodging the regime or compelling it to change its foreign policies. In this case, the U.S. competitive action lacks the force necessary to counter Iranian competition. A competitive action that is an example of a lack of credibility is the U.S. withdrawal from the Joint Comprehensive Plan of Action (JCPOA). With that agreement in 2015, the United States and its allies attempted to impose limits on Iran's potential to develop nuclear weapons capabilities in exchange for sanctions relief. However, less than 2 years after the deal's implementation, President Trump withdrew from it. Among other consequences of scrapping the JCPOA, the withdrawal likely sent a clear message to Iran that American actions and agreements lack credibility

and that negotiations with U.S. officials represent fruitless and capricious efforts. As a result, the Middle East remains a gray zone competitive arena that has seen an increase in Iranian capabilities and influence with a corresponding decrease in U.S. credibility and capability to deter Iranian behavior.

To decisively reverse this trend, the United States can introduce and implement red lines that clearly specify unacceptable Iranian behavior and, critically, enforce them with disciplined lethal actions to ensure Iran pays a proportionate price for unacceptable competitive actions. Implementing red lines with lethal consequences yields two advantages to U.S. competition with Iran. First, it clearly delineates acceptable and unacceptable behavior in the gray zone that would diminish Iran's ability to exploit ambiguity in the Middle East. Identifying such actions as transporting lethal aid shipments to proxy forces, conducting ballistic missile tests, and closing the Strait of Hormuz as unacceptable and punishable behavior begins to clarify expected behavior in U.S.-Iranian competition. Second, imposing disciplined, lethal costs on Iran for unacceptable behavior activates and leverages the main U.S. strength in interstate competition: lethal capabilities. Targeting the Iranian military, the Islamic Revolutionary Guard Corps, or the regime's infrastructure after red line violations would be lethal enough to send a strong message. It would degrade Iranian capability but be sufficiently targeted to impose costs only on the offending security or state apparatus so as not to signal an appetite for large-scale combat. Imposing red lines in the U.S.-Iranian competition enforced with lethal capabilities applied in a targeted fashion represents the best way to effectively compete in a Middle Eastern gray zone, where Iran already holds many advantages, without giving in to hasty and myopic Iran hawk impulses advocating regime change through large-scale combat.

Critics of this recommendation are likely to raise two main issues with the red line and lethal strike competition strategy. First, they are likely to see the

lethal response as inevitably escalating the conflict into just the type of open and large-scale warfare that competitive strategies should be avoiding. However, lethal responses to Iran should not be automatically equated with an invitation to open warfare. It is possible to leverage lethal capabilities in competition without escalating the conflict to open warfare. The U.S. response to the Syrian regime's use of chemical weapons in Ghouta illustrates this point. After the Syrian regime reportedly used chemical weapons in an attack on opposition fighters, U.S. planes bombed regime infrastructure to send a message that such behavior would not be tolerated.¹⁷ In a crisis where U.S. and regime forces have delicately avoided direct confrontation, the bombing did not lead to an escalation in conflict. Additionally, it is worth reiterating that the centerpiece of Iranian competitive activity in the Middle East hinges on proxy forces created and leveraged *specifically because Iran lacks the military resources to support large-scale conflict* with an advanced state. Bluntly, Iran uses proxy forces because it *has to* use them, as it lacks fully developed conventional military capabilities. This reality lessens the chance that targeted lethal strikes against Iran would goad it into a war that it is clearly unprepared to fight.

Second, critics of this proposed strategy will also cite the risks to U.S. and allied forces from the highly capable Iranian proxies in the region. In this line of thinking, lethal strikes from the United States would beget lethal responses from Iranian proxies that could potentially devolve into a violent back-and-forth contest of wills between U.S. allies in the region and Iranian proxies leading to destabilization. But these proxies are already destabilizing the region with relative impunity. Backing Palestinian terrorist groups against Israel, stalling the formation of a legitimate government in Lebanon, forming paramilitary forces in Iraq, and arming a violent insurgency in Yemen show that Iran's destabilizing fingerprints are all over the major regional conflicts. Implementing red lines that carry a lethal response would simply make Iran pay a price for actions it already conducts. Furthermore, Iran's

ability to scale and obfuscate its support to its proxies helps them persist. An up-tick in violent actions from proxies would increase Iran's signature in the region and perhaps fully bring the threat into the open to help coalesce Arab allies against Iran's conduct of violent activities in their own backyard.

At its core, implementing red lines in the Iranian gray zone is a call to re-invigorate American sovereignty in the face of a direct threat. It asserts that the United States has a fundamental right to *directly and unilaterally* challenge direct competitive actions that threaten U.S. interests or allies. Indirect efforts to expand competition with Iran and/or impose meaningful costs on Iranian malign activities do not appear to be working, as Iran nimbly outmaneuvers U.S. efforts to engage the international community. Neither does covert action seem efficient or effective given the fact that U.S. covert actions in 1953 (supporting a coup d'état) ostensibly fomented the mistrust and resentment from Iran that persist to this day and underpin the hostility from the Iranian regime. There are certainly risks involved with implementing red lines with lethal consequences. Striking a sovereign country with military force (even when employed with discipline and scoped to avoid escalation) is no small thing. However, given the competitive advantages Iran currently enjoys in the region and its plethora of malign and destabilizing activities, decisionmakers must ask themselves, "What about the current U.S.-Iran competitive status quo is going well?"

In direct competition between states, lethality still rules the day, and capabilities and competitive overmatch in force-on-force destruction should not be begrimed, marginalized, or discounted. Strategic competition with Iran bears out these truths. Prospects of expanding competition with Iran by leveraging nonmilitary elements of national power are dim from the start given the lack of diplomatic relations between the countries, the overt hostile threats emanating from Tehran, and Iran's tactical reliance on proxy forces in its competitive

approach. The competition paradox and the misalignment in perspectives on the stakes of the competition (wars of necessity versus wars of choice) give Iran further advantages in the competition. The sum of all these factors implies that the United States will not outcompete Iran by trying to expand the competition into realms that are either infeasible or do not activate traditional U.S. overmatch strengths. Rather, introducing the lethality resource into the competition enables the United States to outcompete Iran and compete from a position of strength. To avoid escalating the competition to open warfare, the lethality resource should be introduced in a disciplined capacity that aims to keep competition in the gray zone. Delineating red lines in the gray zone to define acceptable behavior, set expectations, and lay ground rules for competition is a measured way to introduce U.S. competitive advantages that would allow for success in the gray zone while keeping competition beneath large-scale combat. JFQ

Notes

¹ *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), available at <<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>>.

² Ibid.

³ Kenneth Katzman, *Iran's Foreign and Defense Policies*, R44017 (Washington, DC: Congressional Research Service, updated October 8, 2019), available at <<https://fas.org/sgp/crs/mideast/R44017.pdf>>.

⁴ Van Jackson, "Tactics of Strategic Competition: Gray Zones, Red Lines, and Conflicts Before War," *Naval War College Review* 70, no. 3 (Summer 2017).

⁵ "Read a Transcript of Trump and Putin's Joint Press Conference," *Time*, July 31, 2018, available at <<http://time.com/5339848/donald-trump-vladimir-putin-summit-transcript/>>; Yen Nee Lee, "What to Expect from the Crucial G-20 Meeting Between Trump and Xi This Weekend," CNBC, November 30, 2018, available at <www.cnbc.com/2018/11/30/g-20-donald-trump-xi-jinping-meet-to-discuss-us-china-trade-war.html>.

⁶ Anna Fifield, David Nakamura, and Seung Min Kim, "Trump Accepts Invitation to Meet North Korean Leader Kim Jong Un," *Washington Post*, March 8, 2018, available at <www.washingtonpost.com/world/asia_pacific/north-korean-leader-kim-jong-un-has-invited-president-trump-to-a-meeting/2018/03/08/021cb070-2322-11e8-badd-7c9f29a55815_story.html?noredirect=on>; Judson Berger, "Trump Offers to Meet with Iranian President Rouhani, Without Preconditions," Fox News, July 30, 2018, available at <www.foxnews.com/politics/trump-offers-to-meet-with-iranian-president-rouhani-without-preconditions>.

⁷ Connor O'Brien, "Dunford: U.S. Will Work to Re-Establish Deconfliction Effort with Russia in Syria," *Politico*, June 19, 2017, available at <www.politico.com/story/2017/06/19/russia-syria-us-general-joe-dunford-239720>.

⁸ Martin Baccardax, "Stocks Rally on U.S.-China Trade Detente; Trump Blasts Fed Chair Powell," *The Street*, November 28, 2018, available at <www.thestreet.com/markets/stocks-rally-on-u-s-china-trade-detente-trumps-feds-chair-powell-on-blast-14793893>.

⁹ Joseph F. Dunford, Jr., "The Character of War and Strategic Landscape Have Changed," *Joint Force Quarterly* 89 (2nd Quarter 2018).

¹⁰ Ronald Sprang, "Russia in Ukraine 2013–2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO, and Media," *Small Wars Journal*, n.d., available at <<https://smallwarsjournal.com/jrnls/art/russia-ukraine-2013-2016-application-new-type-warfare-maximizing-exploitation-cyber-io-and>

¹¹ Tim Starks, "U.S. Indicts North Korean National for Sony Hack, Massive Cyberattacks," *Politico*, September 6, 2018, available at <www.politico.com/story/2018/09/06/justice-department-north-korea-sony-hack-771212>.

¹² Derek Watkins, "What China Has Been Building in the South China Sea," *New York Times*, October 27, 2015, available at <www.nytimes.com/interactive/2015/07/30/world/asia/what-china-has-been-building-in-the-south-china-sea.html>.

¹³ Jackson, "Tactics of Strategic Competition."

¹⁴ Afshon Ostovar, *Vanguard of the Imam: Religion, Politics, and the Revolutionary Guard* (New York: Oxford University Press, 2016).

¹⁵ Kenneth N. Waltz, "Why Iran Should Get the Bomb: Nuclear Balancing Would Mean Stability," *Foreign Affairs* 91, no. 4 (July/August 2012), 2–5.

¹⁶ Jackson, "Tactics of Strategic Competition."

¹⁷ Jon Sharman et al., "Syria Strikes—As It Happened: Bashar al-Assad's Chemical Weapons Capability 'Set Back for Years' by Bombing, Pentagon Says," *Independent* (London), April 14, 2018, available at <www.independent.co.uk/news/world/middle-east/russia-us-tensions-live-updates-syria-trump-theresa-may-assad-action-chemical-latest-a8302341.html>.

Combat controller watches as C-17 Globemaster III, assigned to 17th Weapons Squadron, Nellis Air Force Base, Nevada, lands on airstrip in Nevada Test and Training Range during joint forcible entry exercise, June 16, 2016 (U.S. Air Force/Kevin Tanenbaum)



Countering A2/AD in the Indo-Pacific

A Potential Change for the Army and Joint Force

By Hassan M. Kamara

The Commander-in-Chief, Far East, considers amphibious training to have unusual significance and importance in the Far East Command since the nature of troop dispositions and geography in the theater are such that a continuous requirement exists for the training of troops in over-water movement.

—LETTER FROM GENERAL HQ, FAR EAST COMMAND TO ACOS G3 OPERATIONS,
HEADQUARTERS DEPARTMENT OF THE ARMY, APRIL 3, 1950

The nature of troop dispositions coupled with the expanse of ocean and numerous islands scattered in the Indo-Pacific region compels the redevelopment of conventional forcible-entry amphibious capability in the U.S. Army for deployment and maneuver. As Commander-in-Chief Far East, General Douglas MacArthur made this assessment over half a century ago, but it deserves intellectual inquiry and dialogue in the contemporary period based on the growing strategic competition and potential for conflict between the United States and its allies and China in the Indo-Pacific. Furthermore, this assessment deserves contemplation based on the Army's ongoing conceptualization of multidomain formations to help future joint force commanders apply the Service's capabilities across all domains, thereby

Major Hassan M. Kamara, USA, is an Officer in the U.S. Army Acquisition Support Center. He recently served on the Army Future Studies Group.



Paratroopers of 2nd Brigade Combat Team, 82nd Airborne Division, conduct joint forcible entry operation during brigade's Mungadai event, on Fort Bragg, North Carolina, April 5, 2016 (U.S. Army/Jason Hull)

presenting multiple and compounding dilemmas for an adversary.¹

A conflict with China in the Indo-Pacific region will most likely involve regional access-denial efforts by China, resulting in a counter-antiaccess/area denial (A2/AD) campaign by the United States and its allies. U.S. joint doctrine anticipates the possibility of engaging in a counter-A2/AD campaign and mandates that “the Armed Forces of the United States must be capable of deploying and fighting to gain access to geographical areas controlled by forces hostile to U.S. interest.”² U.S. forces conduct joint forcible entry operations to gain and maintain access to areas against armed opposition.

The redevelopment of conventional forcible-entry Army amphibious forces will enhance the joint forcible entry capability and capacity of U.S. forces in a potential counter-A2/AD campaign against China in the Indo-Pacific by enabling commanders to deploy and

maneuver the U.S. military’s decisive ground force (the Army) through the maritime domain.³ This proposed change is congruent with the mission of the Army as a component of the joint force. According to Army Doctrinal Publication 1, the Army’s mission is “to fight and win the Nation’s wars through prompt and sustained land combat, as part of the joint force.”⁴ Strategic and tactical mobility are inherent to the Army’s mission, and amphibious operation—as a basic means of deploying and maneuvering Army forces—is vital to the accomplishment of the Army’s mission and its role in the joint force.

It bears emphasizing that the Army has amphibious-capable logistics forces that support joint operations (for example, Joint Logistics Over-the-Shore). However, the Service lacks conventional (regular Army, non-special operations) combat arms formations that are organized, trained, and equipped to deploy

and fight as landing forces in joint forcible entry amphibious operations.

Landing forces are central to amphibious operations. In fact, Joint Publication (JP) 3-02, *Amphibious Operations*, defines an *amphibious operation* as “a military operation launched from the sea by an amphibious force (AF) embarked in ships or craft with the primary purpose of introducing a landing force (LF) ashore to accomplish the assigned mission.”⁵ Also, a landing force can be comprised of either Army or Marine units.⁶

Justification for Studying Redevelopment

Contemporary advancements in military A2/AD capabilities and regional economic and security trends underscore the need to study this topic and foster dialogue. First, the sophistication of the integrated air defenses of America’s potential near-peer adversaries makes the contemporary construct of air superiority

as a condition for deploying and maneuvering ground forces unrealistic in future counter-A2/AD operations. The U.S. Army Training and Doctrine Command (TRADOC) acknowledges the challenge posed by modern A2/AD capabilities and argues that “integrated air defense networks complicate joint operations because hidden, lethal, and dispersed air defenses can allow the enemy to establish air superiority from the ground and take away an essential condition for effective joint force operations.”⁷ This anticipated contest in the air domain, and the potential that the United States could lose its forward bases early in a Chinese A2 campaign, precipitate the need to find ways and means of deploying and maneuvering decisive ground forces through potential corridors of opportunity in the maritime domain.

Contemporary economic and security affairs in the region further underscore the need to study this topic and foster dialogue. Armed conflict between the United States and its allies and China in the Indo-Pacific is likely because China views the South China Sea as a long-term resource vital to meeting its needs and so seeks to control it. This is evident in China’s ongoing construction and force buildup on artificial islands and its armed maritime confrontation with other nations over its appropriation of islands. Geoffrey Till concurs and writes that the South China Sea is a “stock resource” that China sees “as an economic resource vital to its future prosperity” because of the oil, gas, and fish that will support its growing energy and human needs.⁸ Robert Kaplan writes that “at some point, China is likely to, in effect, be able to deny the U.S. Navy unimpeded access to parts of the South China Sea.”⁹ This will precipitate conflict with the United States and its allies in the Indo-Pacific.

Concepts and Framework of Analysis

Articulating the concepts and the framework used for the ensuing analysis is necessary to foster understanding. The concepts discussed include A2/AD, the Joint Operational Access Concept (JOAC), and cross-domain synergy.

A2/AD. Antiaccess is described in the 2012 JOAC as “those actions and capabilities, usually long range, designed to prevent an opposing force from entering an operational area.” The JOAC differentiates antiaccess from area denial. It states that “area denial refers to those actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within the operational area.”¹⁰

The JOAC expects U.S. adversaries will use A2/AD strategies to offset U.S. strategic superiority in multiple domains, and it presents conceptual alternatives to counter them. In the Indo-Pacific, the joint force should expect China to employ an A2/AD strategy that will challenge theater access and freedom of maneuver in a potential conflict. Based on the ability of U.S. adversaries to challenge the joint force’s legacy counter-A2/AD capabilities, TRADOC writes that “the joint force should anticipate disrupted deployment and sustainment operations and degraded effectiveness of the standoff targeting and strikes currently required to gain access and seize the initiative.”¹¹

The 2012 JOAC. The 2012 JOAC describes how the U.S. military envisions its response to emerging A2/AD capabilities of potential adversaries, who seem to view the latter as a preferred method to counter U.S. strategic superiority across domains. Through its central thesis of cross-domain synergy and its principles or precepts, “the JOAC describes how the future joint forces will achieve operational access in the face of such strategies [anti-access and area denial].”¹²

Cross-Domain Synergy. The concept of cross-domain synergy outlined in the 2012 JOAC advocates the “complementary” versus the merely “additive” employment of joint force capabilities to optimize exploitation of the asymmetric advantages inherent in each Service’s capabilities.¹³

The Analytical Framework. The concept of cross-domain synergy as presented in the 2012 JOAC rests on certain precepts intended to help guide thinking and planning for future counter-A2 campaigns. The following analysis uses a selection of these precepts as a lens or

rubric to highlight how the redevelopment of forcible-entry Army amphibious forces would enhance the joint forcible entry capability and capacity of U.S. forces in a possible counter-A2/AD campaign against China in the Indo-Pacific.

Since these precepts are inherently oriented toward meeting the challenges that will be presented to U.S. joint forces by the A2 campaign of a potential peer adversary like China, their use as units of analysis is appropriate. In other words, these precepts are an excellent lens to highlight and appreciate the potential utility of the Army redeveloping conventional forcible-entry amphibious forces to enhance the joint force. The following are the selected precepts of operational access—highlighted in the 2012 JOAC—that comprise the units of analysis for this study:

- Seize the initiative by deploying and operating on multiple, independent lines of operations.
- Exploit advantages in one or more domains to disrupt enemy A2/AD capabilities in others.
- Maneuver directly against key operational objectives from strategic distance.¹⁴

The Precepts

Through the lens of the following precepts of operational access, it is conceivable that the redevelopment of conventional forcible-entry Army amphibious forces will enhance the joint forcible entry capability and capacity of U.S. forces in a potential counter-A2/AD campaign against China in the Indo-Pacific.

Seize the Initiative by Deploying and Operating on Multiple, Independent Lines of Operations. The redevelopment of conventional forcible-entry Army amphibious forces will enhance the joint force’s capability and capacity to mount multiple lines of operations across domains. The latter can compound the number of avenues of approach an enemy has to defend in its A2 campaign. The JOAC concurs and posits that “operating on multiple lines in multiple domains simultaneously can help joint forces to

seize the initiative by overloading the enemy's ability to cope.”¹⁵

During his 1944 World War II Pacific campaign, General MacArthur successfully seized Saidor, New Guinea, from the Japanese by deploying Army, joint, and allied forces on multiple lines of operations across domains. His combat report following the seizure of Saidor proves this:

We have seized Saidor on the north coast of New Guinea. Lit a combined operation of ground, sea and air forces, elements of the Sixth Army landed at three beaches under cover of heavy air and naval bombardment. The enemy was surprised both strategically and tactically and the landings were accomplished without loss. The harbor and airfields are in our firm grasp. Enemy forces on the north coast between the Sixth Army and the advancing Australians are trapped with no source of supply and face disintegration and destruction.¹⁶

Exploit Advantages in One or More Domains to Disrupt Enemy A2/AD Capabilities in Others. Growing conventional forcible-entry amphibious capability in the Army will enable joint force commanders to deploy and maneuver the Service’s decisive ground forces through the maritime domain, not just the air domain, which creates a dilemma for an adversary’s A2/AD campaign planning. This transformation will provide an asymmetrical advantage critical for maneuvering against enemy positions on the many disconnected land masses that will constitute objectives in a potential counter-A2/AD campaign against China. The British experience in the 1982 Falkland Islands campaign is instructive in this regard.

Following its full occupation of the Falkland Islands on April 2, 1982, the Argentinian military developed an integrated air defense system in and around Port Stanley with the aid of an AN/TPS-43 Search radar and a command, control, and communications center (*Centro de Información y Control*). According to Rodney Burden and his co-authors, Argentinian forces deployed several batteries of antiaircraft guns, a Roland

surface-to-air missile unit, and several units of the Shorts Blowpipe and SA-7 Grail man-portable air-defense systems.¹⁷

British military planners were compelled to exploit the Royal Navy’s capabilities in the maritime domain for deployment and decisive ground maneuver because the Argentine air defense threat precluded airborne forcible-entry operations. Additionally, there was no host nation bordering the Falkland Islands that could be used for forward staging and maneuver. Michael Clapp, the commander of the British Amphibious Task Group at the time, writes that quite early in their preparation, British military planners appreciated the disconcerting fact that “there would be no ‘host-nation’ and we would therefore have to offload (possibly during the opposed landing always considered so unlikely by the Government), protect ourselves and deploy forward using our own assets and fuel.”¹⁸

Given the mass or troop strength of Argentinian forces on the Falkland Islands, retaking them required the decisive ground forces of the British army in addition to Royal Marine commando forces. This understanding required deploying both Royal Marine commando forces and the non-amphibious, decisive ground forces of the British army into a maritime-centric theater where the enemy was contesting access by air and sea. Michael Clapp writes that “it was clear . . . that merchant ships would be required and that the 3rd Commando Brigade, Royal Marines, would be enhanced by further Army forces.”¹⁹

Clapp’s statement compels contention with a major counterargument to redeveloping forcible-entry amphibious capability in the U.S. Army for employment in the Indo-Pacific, which is that the amphibious capability of the U.S. Marine Corps is prodigious enough to preclude the need for complementary amphibious capability in the Army. This counterargument indirectly suggests that redeveloping forcible-entry amphibious capability in the Army can make it duplicative and therefore capable of replacing the Marine Corps. This suggestion is groundless because the Marine Corps has

a unique role as America’s elite light expeditionary ground combat force, a role for which the Army, with its greater mass for sustained ground combat operations, is ill suited. The transformation proposed in this article is not targeted at having the Army usurp the role of the Marine Corps but rather at giving future U.S. joint force commanders and planners the ability to deploy and maneuver the Army through temporary maritime corridors of opportunity provided by the Navy to apply its unrivaled capacity for sustained ground combat in the Indo-Pacific.

The counterargument that the amphibious capability of the Marine Corps is prodigious enough to preclude the need for complementary amphibious capability in the Army also fails to take into account the potential for China, like Argentina in the Falklands War, to field forces with capabilities and such mass that it becomes necessary to employ the Army for its mass and endurance in ground combat. This counterargument also neglects the possibility that an adversary may widely distribute its forces among the many disconnected land masses in the Indo-Pacific (consider Japan in the World War II Pacific campaign) to necessitate employing the Army’s decisive ground forces as part of a joint and allied effort to dislodge them.

The British experience in the Falklands campaign shows that in a counter-A2/AD campaign, particularly in a maritime-centric region like the Indo-Pacific, the complementary versus the merely additive employment of joint force capabilities is critical to optimal exploitation of the asymmetric advantages inherent in each Service’s capabilities. The British complemented the amphibious commando forces of the Royal Marines with shipborne army paratroopers to fully exploit the Royal Navy’s sea control for deployment and decisive ground maneuver against Argentine forces.

Maneuver Directly Against Key Operational Objectives from Strategic Distance. Redeveloping forcible-entry amphibious capability in the Army will afford joint force commanders the flexibility of deploying America’s decisive ground forces directly into combat from the U.S. mainland and other overseas



Marines take new Amphibious Combat Vehicle out for open-ocean low-light testing at Del Mar Beach on Marine Corps Base Camp Pendleton, California, December 17, 2019 (U.S. Marine Corps/Andrew Cortez)

bases—thereby complicating enemy defensive preparations by wielding an Army that is not tied to fixed forward bases or restricted solely to deployment and maneuver through the air domain (for example, airborne forced entry). According to the 2012 JOAC, “some elements of the joint force will operate directly against key objectives from points of origin or other points outside the theater without the need for forward staging.”²⁰ The JOAC cautions that the assured regional access afforded by U.S. forward bases can be degraded by attacks on those bases and consequently “calls for some elements of a joint force to maneuver against key operational objectives directly from ports of embarkation.”²¹

According to a 2015 RAND study of U.S.-China military capabilities and capacity in simulated Taiwan and Spratly Islands campaign scenarios, the Chinese military will be able to contest U.S. air superiority through the use of conventional precision standoff weapons and

airpower against critical U.S. forward bases like Kadena Air Force Base, Japan, and Andersen Air Force Base, Guam. The study’s “analysis shows that China’s conventional missile forces have expanded their capabilities over the past 15 years to the point that the PLA [People’s Liberation Army] can now contest U.S. air base operations within roughly 1,500 km of Chinese territory. This capability will indirectly impinge on a much larger range of U.S. capabilities, complicating the air superiority battle.”²²

The British army’s experience in the 1982 Falklands War offers insight on the subject of maneuvering directly against key operational objectives from a strategic distance. Given that the airspace over the South Atlantic was contested by the Argentine air force, and the objective was an island without a land-bordering “host nation,” the British army had to deploy and maneuver directly against operational objectives in the Falkland Islands from the United Kingdom using maritime

corridors facilitated by the Royal Navy’s control of the sea. Subsequently, the British military hastily requisitioned several merchant ships taken up from trade (STUFTs) to transport ground forces to the Falkland Islands. Many STUFTs were hurriedly retrofitted for transporting Army and Marine commando troops. Among the STUFTs was the North Sea ferry MV *Norland*, which transported 840 paratroopers from the British army’s Second Battalion, Parachute Regiment.²³ Another STUFT used to move troops in the counter-A2 campaign was the SS *Canberra*, a cruise ship.

The Way Ahead: Recommendation

There are many considerations inherent in redeveloping conventional forcible-entry amphibious capability in the Army. Two broad yet critical considerations are examined herein. First, as part of any effort to redevelop conventional forcible-entry amphibious capability

in the Army, this Service and the joint force as a whole should develop an intellectual foundation in the form of an operational concept that will facilitate force development, resourcing, and overall force management decisions. As part of this effort, the Army should review and update its legacy doctrine for amphibious operations in coordination with the Navy and Marine Corps.

In the 1960s, the now inactive Field Manual 31-12, *Army Forces in Amphibious Operations (The Army Landing Force)*, provided Army commanders and planners “the fundamental principles, doctrine, and procedures relative to the U.S. Army component of an amphibious task force.”²⁴ Obsolete doctrinal documents like this are worth revisiting to help rebuild the intellectual foundation of Army amphibious operations as part of the joint force.

Working in concert with the Navy and Marine Corps, the Army should consider identifying, training, and qualifying two brigade combat teams (BCTs) to operate as landing forces in an amphibious task force because these teams generally possess the command, ground maneuver, aviation, and logistics elements that will make them operationally effective as a landing force. For operational flexibility, one of the BCTs should be capable of conducting ship-to-shore movement by helicopter (air assault) and the other by surface (landing craft).

Additionally, selecting a BCT to serve as a landing force in joint forcible entry amphibious operations will ensure the Army provides the joint task force commander the doctrinally prescribed suite of combat and combat Service support capabilities. JP 3-02, *Amphibious Operations*, mandates that “the Army maneuver battalion, brigade, division, or corps . . . be task-organized with appropriate combat and combat Service support capabilities.”²⁵

The redevelopment of conventional forcible-entry Army amphibious forces in the contemporary period could benefit the Army and the joint force in a potential counter-A2/AD campaign against China in the Indo-Pacific. Currently, the joint

force’s ability to deploy and maneuver America’s decisive ground force against an adversary like China in a contested maritime-centric region like the Indo-Pacific is limited to transit through the land and air domains. Redeveloping forcible-entry amphibious capability in the Army will afford future joint force commanders the flexibility of deploying and maneuvering the Army’s decisive ground forces from theater and strategic distances through temporary corridors of sea control afforded by the Navy. This will increase the overall cross-domain synergy of U.S. forces in a potential counter-A2/AD campaign against China in the Indo-Pacific. In his work on A2/AD, Sam Tangredi highlights the value of cross-domain synergy and writes that “militaries that can obtain cross-domain synergy are simply better, more capable [ones].”²⁶ JFQ

Notes

¹ U.S. Army Training and Doctrine Command (TRADOC), Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, December 6, 2018), iii, available at <www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf>. The Army’s evolving concept of multidomain operations is congruent with the joint force’s efforts to integrate U.S. capabilities to fight in “all domains.” Speaking on changes in the character of war and the global strategic landscape, General Joseph F. Dunford, Jr., emphasized that the “future force must remain competitive in ‘all domains,’ deny adversaries’ ability to counter our strengths asymmetrically, and retain the ability to project power at a time and place of our choosing.” See “Gen. Dunford: The Character of War & Strategic Landscape Have Changed,” *DOD Live*, April 30, 2018, available at <www.dodlive.mil/2018/04/30/dunford-the-character-of-war-strategic-landscape-have-changed/>.

² Joint Publication (JP) 3-18, *Joint Forcible Entry Operations* (Washington, DC: The Joint Staff, 2018), vii, available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_18ch1_pa.pdf?ver=2018-07-03-125841-997>.

³ *Decisive ground force* refers to the Army’s unrivaled capacity (the combination of its superior mass, lethality, and sustainment infrastructure) for sustained (long-term) ground combat operations.

⁴ Army Doctrinal Publication 1, *The Army* (Washington, DC: Headquarters Department of the Army, September 2012), I-8, available at

<<https://caccapl.blob.core.usgovcloudapi.net/web/repository/doctrine/adp1.pdf>>.

⁵ JP 3-02, *Amphibious Operations* (Washington, DC: The Joint Staff, August 10, 2009), xi, available at <www.jag.navy.mil/distrib/instructions/JPub3-02AmphibiousOps.pdf>.

⁶ Ibid., II-7.

⁷ *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century, 2025–2040*, version 1.0 (Fort Eustis, VA: TRADOC, December 2017), available at <[www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20\(1\).pdf](http://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf)>.

⁸ Geoffrey Till, *Seapower: A Guide for the Twenty-First Century* (New York: Routledge, 2013), 319.

⁹ Robert D. Kaplan, *Asia’s Cauldron: The South China Sea and the End of a Stable Pacific* (New York: Random House, 2015), 15.

¹⁰ *Joint Operational Access Concept (JOAC)*, version 1.0 (Washington, DC: Department of Defense, January 17, 2012), available at <archive.defense.gov/pubs/pdfs/JOAC_Jan%202012_Signed.pdf>.

¹¹ *Multi-Domain Battle*.

¹² JOAC.

¹³ Ibid.

¹⁴ Ibid., 17.

¹⁵ Ibid., 20.

¹⁶ *Reports of General MacArthur, The Campaigns of MacArthur in the Pacific*, vol. 1 (Washington, DC: U.S. Army Center of Military History, 1994), 132, available at <history.army.mil/html/books/013/13-3/CMH_Pub_13-3.pdf>.

¹⁷ Rodney A. Burden et al., *Falklands: The Air War* (London: British Aviation Group, 1986), 17–18.

¹⁸ Michael Clapp and Ewen Southby-Tailyour, *Amphibious Assault Falklands: The Battle of San Carlos Water* (Annapolis, MD: Naval Institute Press, 1996), 35.

¹⁹ Ibid., 25.

²⁰ JOAC, 23.

²¹ Ibid., 19.

²² Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017* (Santa Monica, CA: RAND, 2015), 45, available at <www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR392/RAND_RR392.pdf>.

²³ Ibid., 64–65.

²⁴ Field Manual 31-12, *Army Forces in Amphibious Operations (The Army Landing Force)* (Washington, DC: Headquarters Department of the Army, March 1961), 4.

²⁵ JP 3-02, II-7.

²⁶ Sam J. Tangredi, *Anti-Access Warfare: Countering A2/AD Strategies* (Annapolis, MD: Naval Institute Press, 2013), 157.



General U.S. Grant, ca. 1855–1865
(Library of Congress/Brady-Handy)

Learning the Art of Joint Operations

Ulysses S. Grant and the U.S. Navy

By Harry Laver

In February 1862, Major General George B. McClellan sent his appreciation to Brigadier General Ulysses S. Grant and Flag Officer Andrew H. Foote of the U.S. Navy for the recent capture of Fort Donelson on the Cumberland River in Tennessee.¹ Ten days earlier, the two officers and their commands had captured Fort Henry on the Tennessee River, just 10 miles to the west. Confederate generals had counted on the two forts to stop Federal forces from moving south along the two rivers, both natural avenues of advance—the Tennessee reaching into the piney woods of northeast Mississippi, the Cumberland bending southeast toward Tennessee's Confederate state capital of Nashville. With those fortifications now in Union hands, the heart of the western Confederacy was laid open to further operations by U.S. forces.

McClellan's commendation acknowledged that the operations' success resulted from cooperation between Grant's land and Foote's naval forces. While the term *joint operations* had not yet become part of the profession's language, the concept was anything but new, as centuries of warriors had recognized the advantages of soldiers and sailors working together. In a practical way, the two Services have always been complementary, with armies fighting on land, seizing and occupying terrain, while navies provided transportation, sustainment, and, when possible, fire support. Effectively conducting such operations, however, presents challenges not encountered by a single Service operating alone. Among the inter-Service gaps to be bridged are differences in doctrine, technology, weapons, planning, and more abstract factors such as culture. As Milan Vego points out, joint operations are inherently complex "because of the need to sequence and synchronize the movements and actions of disparate force

Dr. Harry Laver is a Professor of Military History at the U.S. Army Command and General Staff College.

elements. Sound command and control can be especially challenging.”²

Vego’s observation is just as applicable to the Civil War period as it is today, if not even more so. In the mid-19th century, the principle of unity of command had not been defined, at least not formally. Today, that concept is meant to mitigate the confusion and complexity of joint operations—as Joint Publication 3-0, *Joint Operations*, points out—by assigning “a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose.”³ In the 1860s, however, without such a formal directive, officers had to rely on cooperation developed through personal relationships to make joint operations work. Over the course of the war, Grant learned the art of joint operations by working with his naval counterparts to form relationships built on trust, honesty, mutual respect, and a commitment to the ultimate objective of winning the war. Such relationships do not occur by chance, as Grant learned working with Foote. Grant’s experiences in learning to cooperate with the Navy are a reminder that interpersonal relationships, inter-Service respect, and learning from one’s missteps are essential ingredients of effective joint operations.

First Battles, First Missteps

In the summer of 1861, Grant was barely back in uniform when he began working with elements of the Navy’s Western riverine fleet. During a futile search for Confederate officer Thomas Harris in July 1861, naval transports ferried Grant’s force across the Mississippi River from Illinois to Missouri. Two months later in early September, Grant and his troops occupied Paducah, Kentucky, the first Federal presence in the Bluegrass State; their transit from Cairo, Illinois, across the Ohio River was facilitated by two gunboats and three steam transports of Foote’s command.⁴

As summer turned to fall, Grant and naval commanders continued to communicate about simple matters such as positioning gunboats and reconnaissance operations around the confluence of

the Ohio and Mississippi rivers. Their exchanges were professional, typically couched as requests rather than as orders. The exception was a minor dispute over control of the *Graham*, a “wharf boat” used for storing supplies. Grant, citing a lack of sufficient storehouses on land, first appropriated it, thereby initiating an exchange with Foote over who most needed the boat. Neither man was prepared to concede, so Foote appealed to the senior officer in the area, General John C. Frémont, for arbitration.

Resolution came when Foote and Grant together, or so it seemed, worked out a compromise to divide the ship’s space in half. Writing to Grant, Foote confirmed that the Army “will retain one half of the Boat, offices included, and we will endeavor to get on with the other half,” all “to promote conjointly the highest interest of the government.” The spirit of cooperation, however, had not in fact prevailed, as Foote revealed in a subsequent letter to Washington, DC, when he noted that Grant “would not give a place assigned . . . to our store, had it not been a positive order from Genl. Frémont.” Still new to command, and especially inexperienced in working with the Navy, Grant had yet to learn that his effectiveness as an Army commander was dependent on a working relationship with his naval peers, who controlled essential capabilities the Army itself could not provide. Nevertheless, in the midst of this tug of war, Foote wrote to naval secretary Gideon Welles that “I am on good terms with the army officers.” Less than a month later, Grant would make another misstep with Foote, from which the Soldier would come to appreciate the necessity of open communication with the Sailor.⁵

During the movement to and from the Battle of Belmont, Missouri, on November 7, 1861, six steamers transported Grant’s infantry across the Mississippi, while the gunboats *Tyler* and *Lexington* provided fire support. In the weeks leading up to the battle, Grant and Commander Henry Walke worked closely on the deployment of watercraft on the Mississippi River, especially the gunboats, mostly around Cairo, Illinois. When

Grant decided to move against Belmont, however, communication with Walke broke down. The naval commander first learned of the operation verbally late in the evening of November 6, less than 12 hours before movement began. Grant’s written orders then arrived around 3:00 A.M., instructing Walke that the transit of troops would begin a mere 3 hours later. Walke set the Navy in motion with all possible speed, but one can imagine his frustration at the lack of prior notice. Grant, perhaps overly concerned about operational security, had withheld details until the last minute even from some of his own officers.⁶

Despite the short notice, Walke and his Sailors all performed proficiently and professionally before, during, and after the battle, landing the Army just north of Belmont, providing supporting artillery fire, and facilitating the Soldiers’ escape when the Confederates counterattacked. Walke was proud of his command, noting, “with what zeal and efficiency they all performed,” in spite of being “apparently new material.” Grant agreed with Walke’s self-assessment, complimenting the Navy’s “most efficient service. . . . They engaged the enemy’s batteries . . . and protected our transports throughout.” Importantly, Grant shared that praise with Walke and his Sailors, acknowledging the Navy’s participation and their essential contribution to the Army’s success.⁷

Captain Foote, Walke’s commanding officer, however, was less than pleased with how Grant conducted the operation—specifically, the lack of communication between Grant and himself as the senior naval officer in the area. In his report to Secretary Welles, Foote complimented the performance of the Army, stating that the horses of both Grant and General John McClernand had been hit during the fight, evidence of the officers’ courage. Nevertheless, Grant had failed to honor their agreement:

to inform me . . . whenever an attack upon the enemy was made requiring the cooperation of the gunboats. . . . No telegram was sent me, nor any information given by General Grant when the movement upon



Commodore Andrew H. Foote, ca. 1860–1865 (National Archives and Records Administration/Mathew Brady)

Belmont was made. . . . I deeply regret the withholding of this information from me, as I ought not only to have been informed, in order that I might have commanded the gunboats, but it was a want of consideration toward the Navy, a cooperating force with the army on such expeditions.⁸

Foote concluded by asking Welles either to send a more senior naval officer who would have “immunity from the orders of brigadier-general down to lieutenant-colonel, who are inexperienced in naval matters” or to promote him to the rank of flag officer, equivalent to Grant’s rank of brigadier. Welles recognized that Foote’s request was well-founded and necessary; the promotion came on November 13.⁹

Foote was correct in his criticism of Grant, not only for failing to follow through on their agreement, but also for a lack of consideration for a fellow officer and sister Service. Either through belated self-awareness or the prompting of another—Grant left no record of the incident—the general sought out Foote shortly after the battle and “expressed his regret that he had not telegraphed as he had promised, assigned as the cause that he had forgotten it, in the haste in

which the expedition was prepared, until it was too late for me to arrive in time to take command.” The explanation was plausible, and one that Foote accepted. Grant took responsibility for the error and, more important, learned a valuable lesson about the necessity for cooperation with the Navy.¹⁰

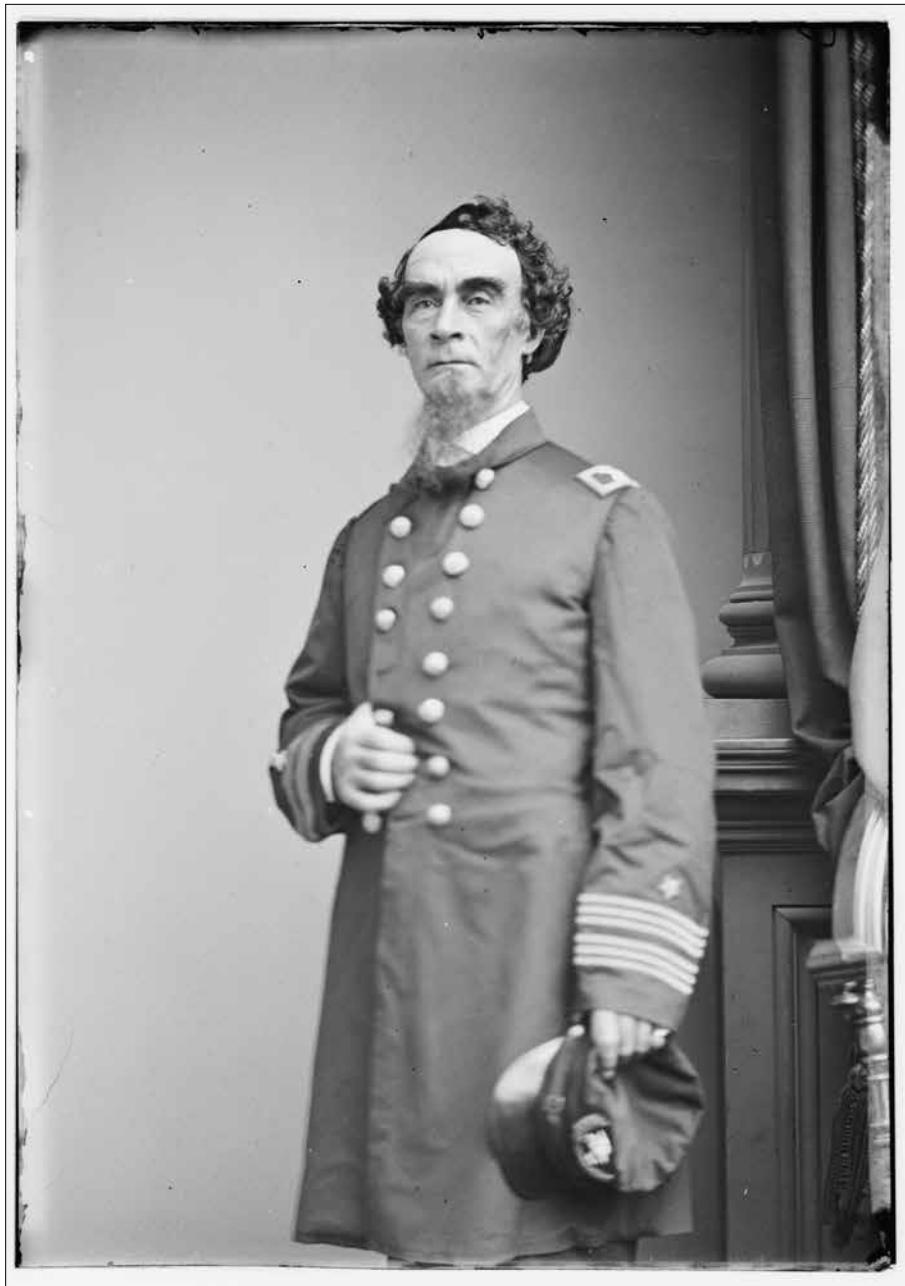
Perhaps it was Foote’s promotion to flag officer, Grant’s new appreciation for the Navy and its capabilities, or a combination of both, that prompted Grant to modify his interactions with his naval colleagues following the battle at Belmont. From late 1861 into the first weeks of the new year, Grant’s relationship with Foote and Walke was professional, respectful, open, and honest. *Consultation* was the watchword for inter-Service interaction.¹¹

Fortunately for the Union, Grant and Foote shared a commitment to the cause of which both were a part, recognizing that cooperation would advance the day of final victory. Foote believed that the Army and Navy “were like blades of shears—united, invincible; separated, almost useless,” a philosophy Grant was coming to share. And perhaps because Grant was still learning the lessons of joint operations, Foote was willing to forgive errors of initiative and aggression.

The coming campaign against Fort Henry and Fort Donelson would demonstrate that Grant had indeed learned something over the previous months and that his approach for dealing with the Navy had matured.¹²

Lessons Learned, Lessons Applied

The improved relationship between the Services paid off in mid-January when one of Grant’s subordinates, Brigadier General Charles F. Smith, reported that Fort Henry, the Confederates’ safeguard of the Tennessee River, was vulnerable. Reacting to Smith’s assessment, on January 23 Grant headed to St. Louis where he proposed to Major General Henry Halleck, the senior officer in the region, an expedition in conjunction with the Navy to seize Fort Henry. Halleck, Grant recalled, received him with “little cordiality,” and within a few minutes “cut short” the interview, “as if my plan was preposterous.” Grant returned to Cairo “crestfallen” but not cowed. The following day he telegraphed Halleck, “With permission I will take Fort McHenry [sic] on the Tennessee and hold and establish a large camp there.” Given the rebuff he had



Captain Henry Walke, ca. 1861–1865 (Library of Congress/Mathew Brady)

just received at the hands of Halleck, why would Grant have any expectation of a different response? Because this time, he had Foote on his side. Grant wrote later that he and Foote had “consulted freely upon military matters and he agreed with me perfectly as to the feasibility of the campaign up the Tennessee.” Arriving the same day as Grant’s telegram, a note came from Foote, informing Halleck that “General Grant and myself are of the opinion that Fort Henry . . . can be carried . . . and

permanently occupied. Have we your authority to move?” With Foote now backing the idea, Halleck looked past his reservations about Grant to see the soundness of the proposal, and shortly after not only gave his blessing but also claimed to have originated the idea: “I made the proposition to move on Fort Henry first to General Grant.”¹³

With approval secured, on February 3 the joint force headed south on the Tennessee River. Three days later, Foote informed Secretary Welles that

after a “severe and closely contested action” between his gunboats and the Confederate batteries, “the rebel flag was hauled down” as the fort’s garrison surrendered to the U.S. Navy. Grant’s infantry arrived shortly after to occupy the fort and take charge of the prisoners. For his part, Grant commended Foote’s success. Walke recalled that once the fort was secure, Grant joined him on the USS *Carondelet* and “complimented the officers of the flotilla in the highest terms for the gallant manner in which they had captured Fort Henry.” Grant then notified Halleck’s headquarters that “in little over one hour all the batteries were silenced and the fort surrendered.” The Army commander showed no sign of jealousy or resentment, but instead saw the Navy’s victory for what it was—a Union victory—and that was something he would celebrate, no matter who received the credit.¹⁴

The working relationship that Grant and Foote had cultivated over the preceding months had now borne fruit. Their like-minded approach to fighting the war and spirit of “consultation” had won a significant victory, and that shared perseverance would now carry them forward, specifically 10 miles to the east, where the Confederate garrison at Fort Donelson offered the next prize.

As Union infantry were settling into Fort Henry on February 6, Grant and Walke continued to cooperate by sending a joint force south on the Tennessee River to destroy a bridge on the critical Memphis, Clarksville & Louisville Railroad. The primary objective, however, was Fort Donelson, tantalizingly close on the Cumberland River where it blocked Federal access to Nashville. “I was very impatient to get to Fort Donelson,” Grant later wrote, wanting to strike before the arrival of Confederate reinforcements. He made his intentions clear when he told Halleck that he intended to move immediately on Donelson, a determination with which Foote could sympathize and willingly support, if not for the practical concerns of needing to refit his small fleet because of the damage suffered in the duel for Fort Henry.¹⁵

To undertake those repairs, Foote and most of his force returned to Cairo, where on February 10 he received a request from Grant to hurry along whatever boats he could to Fort Donelson as soon as possible. Revealing his frustrations with the campaign's waning momentum, Grant wrote that he had "been waiting patiently for the return of the gunboats." "I feel that there should be no delay" in moving on Donelson, he continued, but conceded the advantages, if not the necessity, of a joint operation: "I do not feel justifiable in going without some of your boats to co-operate." If it would help "expedite matters," Grant offered some of his artillerymen "to serve on the gunboats temporarily." Concluding, he wrote, "please let me know your determination in this matter and start as soon as you like. I will be ready to co-operate at any moment." Brigadier General Lewis Wallace, one of Grant's division commanders, confirmed Grant's hesitancy to move without Foote when he wrote that Grant "relied upon Flag-Officer Foote and his gun-boats, whose astonishing success at Fort Henry justified the extreme of confidence."¹⁶

Despite Grant's impatience, his emphasis on cooperation demonstrates how his manner of dealing with Foote had evolved since the previous November. Evidenced by his offer of men to serve on gunboats, he now understood that to achieve the greatest possible effects, the Army and Navy had to support each other and that he shared in the responsibility for that cooperation. He therefore sought the assistance of a co-equal, recognizing that another Service provided critical capabilities and that the sum of their combined efforts was greater than the individual components. To accomplish the mission, Grant wisely and correctly sought Foote's commitment rather than his compliance.

Foote, who was receiving additional pressure from Halleck to get the gunboats moving up the Cumberland to Donelson, took action almost immediately on receiving Grant's request of February 10. Orders went out to Lieutenant Seth Ledyard Phelps "that all the available gunboats should

immediately proceed up the Cumberland River and in cooperation with the army make an attack on Fort Donelson."¹⁷ Foote made the order despite his own reservations; he confessed to Secretary Welles, "I go reluctantly, as we are short of men. . . . [Nevertheless] I shall do all in my power to render the gunboats effective in the fight, although they are not properly manned."

By February 12, Grant's army had arrived at Donelson and took up positions that pinned the Confederate garrison against the Cumberland River. The Navy arrived the same day in the form of the *Carondelet* and Commander Walke, who ordered "a few shell[s] [thrown] into Fort Donelson to announce my arrival to General Grant." Walke's means of signaling his approach was effective, and the next morning Grant asked him to "advance with your gun boats" to divert Southern attention, while the infantry extended and strengthened its positions around the fort. Walke responded in the affirmative, and at the agreed time his gunners sent into the fort nearly 150 shells, followed by another 45 rounds later in the day. That evening Foote himself finally arrived with five gunboats to supplement the firepower of Walke's *Carondelet*.¹⁸

The next day, February 14, the re-united Army and Navy commanders set their plan in motion. The joint attack, as Grant understood it, "was for the troops to hold the enemy within his lines, while the gunboats should attack the water batteries at close quarters and silence his guns." In short, they sought a repetition of the Fort Henry operation that had proved so successful just a week earlier, but Fort Donelson presented a different challenge altogether with its higher elevation, clear sight lines toward the approaching gunboats, and determined gunners.¹⁹

At 3:00 that afternoon, Foote led forward his four ironclads abreast, with the two wooden gunboats following. In the artillery duel that followed, all the ironclads suffered significant damage, with two being disabled—including Foote's *St. Louis*, which suffered a direct hit on its wheelhouse that killed the

pilot and wounded Foote. The one bit of luck the Sailors had that day was the Cumberland's current carried the damaged vessels away from the Southern batteries rather than deeper into the killing zone. Grant, who observed the fight from the riverbank, wrote of his dismay as he watched Confederate rounds repeatedly find their mark, followed by the withdrawal of Foote's flotilla. Having witnessed the Navy's rebuff if not defeat, he and his Soldiers were "anything but comforted." Facing the likelihood of a lengthy siege as temperatures sank to well below freezing, Grant anticipated having "to intrench my position, and bring up tents for the men or build huts."²⁰

The sun had yet to crest the horizon the next morning when Grant received a note from Foote asking for a meeting aboard his flagship to discuss their course of action given the preceding day's setback. Foote apologized for not traveling himself but explained that his wound prevented ease of movement. Grant immediately set off for the river, and if he had any doubts about the beating the Confederates inflicted on the Navy, seeing the damage to *St. Louis* surely must have convinced him of the intensity of the fight. Once in conversation, Foote explained that the damaged vessels had to return north for repairs before they could join in another attack, an assessment with which Grant immediately concurred. "I saw the absolute necessity of his gunboats going into hospital," Grant recalled, but even with Foote's expectation of returning within 10 days, Grant's fears remained of having to undertake a lengthy siege. Foote sent word to Secretary Welles that after "consultation with General Grant . . . I shall proceed to [Cairo] with the two disabled boats, leaving the two others here . . . to make an effectual attack upon Fort Donelson." Despite the recent failures, both men were determined to take the Confederate stronghold. The only question was whether that would happen sooner or later.²¹

The answer came quicker than either man would have predicted, for as they concluded their meeting, word came that the Confederates had attacked in an attempt to escape Fort Donelson.



Battle of Fort Donelson (Library of Congress/Sarony, Major & Knapp)

Grant's concerns about a long siege thus proved unfounded because, as he later wrote, "the enemy relieved me of this necessity." Upon his return to the front, Grant quickly and correctly assessed the situation, ordering his three divisions to counterattack, and while his decisiveness indicated a degree of courage and confidence, his request to the Navy for assistance suggests the depth of his concern. At about 2:00, he sent a message to the "Commanding Officer Gun Boat Flotilla," being uncertain who was in command since Foote's departure earlier in the day, asking that the gunboats "immediately make their appearance to the enemy. . . . Otherwise all may be defeated. . . . If the Gun Boats do not show themselves it will reassure the enemy and still further demoralize our troops." Understanding the terrific damage the vessels suffered the previous day, Grant made clear the modest assistance he sought: "I do not expect the Gun Boats to go into action, but to make their appearance, and throw shell at long range." Support, any support, was sorely needed.²²

Grant must have wondered how responsive the Navy would be given Foote's absence. Would Foote's subordinates maintain the inter-Service cooperation that the two senior

commanders had established over the preceding weeks, or would they leave Grant and the Army to fend for themselves, a pardonable position given the previous day's losses? Upon receiving Grant's request for assistance, Commander Benjamin M. Dove, now in charge of the naval element at Donelson, did not hesitate, and after quickly surveying his gunboats determined that only the *St. Louis* and *Louisville* were fit to respond. They immediately moved forward, lobbing shells into the midst of the Confederate position, marking the first time in the campaign that the two Services were simultaneously and cooperatively engaged in a fight. The effects of the naval salvos were more psychological than physical but were useful nonetheless. After the battle, Lew Wallace, Grant's Third Division commander, recalled "the positive pleasure the sounds gave me" when the naval guns opened fire. He continued, "That opportune attack by the fleet was, I thought, and yet think, of very great assistance. . . . It distracted the enemy's attention." Grant's counterattack, aided by Dove's timely arrival and the diversion his gunners created, drove the Confederates back into Fort Donelson, where, recognizing the futility of continued resistance, they surrendered the following day. While "Unconditional

Surrender Grant" received most of the credit, this was indeed a victory of effective joint operations.²³

In just 10 days, the Army and Navy, thanks primarily to the close collaboration of their respective commanders, had captured two forts and shattered the Confederates' defensive line on which they had entrusted their Western strategy. The Tennessee and Cumberland rivers now lay open to further exploitation by Union forces, an opportunity both Grant and Foote pursued, culminating in the capture of Nashville on February 25, 1862, the first Confederate state capital to fall to Federal forces.

Mutual Respect and Professionalism

The occupation of Nashville marked the successful conclusion of the campaign, and also the last time Grant and Foote worked directly with one another. They had been together for a relatively brief time, from the fall of 1861 to March 1862, and from the start, Foote was committed to developing a collaborative relationship with Grant and the Army. The naval commander was 16 years older than Grant, a difference in age and perspective that brought greater maturity and appreciation for the effectiveness and necessity of joint operations. Recognizing that personal relations mattered, Foote demonstrated professionalism and respect from the war's beginning, always being liberal with his praise for the Army. In the days after the victory at Fort Donelson, Foote wrote that the "army has behaved gloriously," that they "fought like tigers," and of his relationship with Grant and Union division commander Charles F. Smith, he believed "we are all friendly as brothers." Responding to news of Grant's promotion at the campaign's conclusion, Foote congratulated the new major general with the affirmation that "you have placed your name so high on the pages of your country's history." Grant conveyed a reciprocal sentiment, telling Foote "you are appreciated, deservedly, by the people . . . of this broad country."²⁴

Grant had come to admire Foote, a likeminded warrior who, despite some

significant differences in personality and command style, shared a desire to maintain momentum and the initiative, a belief in unity of effort and the efficacy of joint operations, and a commitment to the Union cause. Their personal relationship, along with Foote's experience and professional wisdom, likely helped Grant grow and mature as a commander. Foote's firm but fair criticism of Grant's failure to communicate at Belmont taught the young general the value and necessity of open communication, along with consideration and respect for peers, including those in the Navy. From that experience Grant left behind a dismissiveness toward the Navy—or, perhaps more accurately, he found an appreciation for the resources and capabilities the sea Service could contribute to a campaign's success. The experiences of Grant and Foote remind us that in an era when there was no joint doctrine, effective inter-Service cooperation and effectiveness depended on mutual respect and professional interpersonal relationships. Today, despite libraries of joint manuals, publications, and doctrine, the same still holds true. JFQ

Notes

¹ Timothy B. Smith, *Grant Invades Tennessee: The 1862 Battles for Forts Henry and Donelson* (Lawrence: University Press of Kansas, 2016), 392.

² Milan N. Vego, "Major Joint/Combined Operations," *Joint Force Quarterly* 48 (1st Quarter 2008), 113.

³ Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 2017), A-2.

⁴ Brooks D. Simpson, *Ulysses S. Grant: Triumph Over Adversity, 1822–1865* (Boston: Houghton Mifflin Harcourt, 2000), 86–87; Report of Brigadier-General Grant, September 6, 1861, *Official Records of the Union and Confederate Navies in the War of the Rebellion* [ORN] (Washington, DC: Government Printing Office, 1908), ser. 1, 22:317. *Editor's note:* All titles for ORN entries have been shortened for this article.

⁵ For examples of general communications, see Grant to Andrew Foote, September 22, 1861, ORN, ser. 1, 22:345; Foote to Grant, September 23, 1861, ORN, ser. 1, 22:346; Grant to Foote, October 1, 1861, in *The Papers of Ulysses S. Grant* [PUSG], ed. John Y. Simon, vol. 3, October 1, 1861–January 7,

1862 (Carbondale: Southern Illinois University Press, 1967–2005), 5; Grant to Henry Walke, October 6 and 7, 1861, PUSG 3:22, 27; Walke to Grant, October 18, 1861, PUSG 3:55–56n; Grant to Walke, October 31, 1861, PUSG 3:99–100. For the exchange relating to the wharf boat, see the exchange of letters, October 17 through November 2, 1861, PUSG 3:46–48n2, 62n; Foote to Gideon Welles, October 23, 1861, ORN ser. 1, 22:376.

⁶ For examples of Grant and Walke's communications, see Grant to Walke, October 6, 7, 9, 22, 1861, ORN 22:362–363, 365, 376; Grant to Walke, November 7, 1861, ORN 22:402; Nathaniel Cheairs Hughes, Jr., *The Battle of Belmont: Grant Strikes South* (Chapel Hill: University of North Carolina Press, 1991), 48–49.

⁷ Report of Walke, November 9, 1861, ORN 22:400–401; Report of Brigadier General Grant, November 17, 1861, ORN 22:405; Henry Walke, "The Gun-Boats at Belmont and Fort Henry," in *Battles and Leaders of the Civil War*, ed. Robert U. Johnson and Clarence Clough Buel, vol. 1, *The Opening Battles* (New York: Century Company, 1887–1888), 361.

⁸ Report of Foote, November 9, 1861, ORN 2:399–400.

⁹ Smith, *Grant Invades Tennessee*, 35.

¹⁰ Report of Foote, November 9, 1861, ORN 2:400.

¹¹ For examples, see Grant to Walke, November 15, 1861; Grant to Foote, December 13, 1861; Grant to Foote, January 2, 1862; Foote to Welles, January 9, 1862, ORN 22:431, 461–462, 482, 489; Grant to Foote, January 9, 1862, in *War of the Rebellion: A Compilation of the Official Records of the Union and Confederate Armies* (Washington, DC: Government Printing Office, 1880–1901), ser. 1, 7:541. Grant also supported naval operations, for example, by ordering out the cavalry to screen a reconnaissance by three gunboats down the Mississippi River toward Columbus, Missouri; see Grant to Brigadier General El-eazer A. Paine, January 6, 1862, PUSG 3:377.

¹² Foote, "Notes on the Life of Admiral Foote," in *Battles and Leaders of the Civil War*, 1:347.

¹³ Charles F. Smith to John A. Rawlins, January 22, 1862, PUSG, vol. 4, *January 8–March 31, 1862*, 91n; Grant to Mary Grant, January 23, 1862, PUSG 4:96; Ulysses S. Grant, *Memoirs and Selected Letters*, ed. Mary D. McFeely and William S. McFeely (New York: Library of America, 1990), 190; Grant to Henry Halleck, January 28, 1862, PUSG 4:99; Foote to Henry Halleck, January 28, 1862, ORN 22:524; Smith, *Grant Invades Tennessee*, 137–140.

¹⁴ Report of Foote, February 7, 1862, ORN 22:538; Grant to Captain J.C. Kelton, February 6, 1862, PUSG 4:157; Walke, "The Gun-Boats," 367.

¹⁵ Grant to Walke, February 7, 1862, PUSG 4:168–169; Grant, *Memoirs and Selected Letters*, 197; Smith, *Grant Invades Tennessee*, 137–138.

¹⁶ Grant to Foote, February 10, 1862, PUSG 4:182; Lewis Wallace, "The Capture of Fort Donelson," in *Battles and Leaders*, 1:412; Smith, *Grant Invades Tennessee*, 137–138.

¹⁷ Halleck to Brigadier General G.W. Cul-lum, February 9 and 10, 1862, ORN 22:577–578; Halleck to Foote, February 11, 1862, ORN 22:582; Foote to Lieutenant S.L. Phelps, February 10, 1862, ORN 22:583; Foote to Welles, February 11, 1862, ORN 22:550.

¹⁸ Grant to Walke, February 13, 1862, PUSG 4:202; Walke to Foote, February 15, 1862, PUSG 4:202–203n; Smith, *Grant Invades Tennessee*, 177–178.

¹⁹ Grant, *Memoirs and Selected Letters*, 202; Smith, *Grant Invades Tennessee*, 244–254.

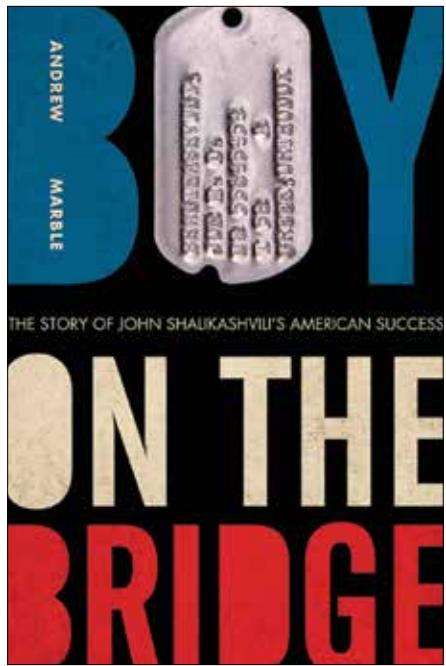
²⁰ Report of Foote, February 15, 1862, ORN 22:585–586; Grant, *Memoirs and Selected Letters*, 202–203.

²¹ Grant, *Memoirs and Selected Letters*, 203; Report of Foote, ORN 22:586.

²² Grant, *Memoirs and Selected Letters*, 204; Grant to Commanding Officer, February 15, 1862, PUSG 4:214.

²³ Benjamin M. Dove to Foote, February 16, 1862, ORN 22:588–589; Testimony of Major-General L. Wallace, ORN 22:589–590; Smith, *Grant Invades Tennessee*, 330–331; Bruce Catton, *Grant Moves South, 1861–1863* (New York: Little, Brown and Co., 1960), 168.

²⁴ Foote to Welles, February 17, 1862, ORN 22:584; Foote to Caroline A. Foote, February 18, 1862, in James M. Hoppin, *Life of Andrew Hull Foote, Rear Admiral United States Navy* (New York: Harper and Bros., 1874), 230–231; Foote to Grant, March 8, 1862, ORN 22:660; Grant to Foote, March 3, 1862, PUSG 4:314. Writing in the 1870s, William T. Sherman remembered the old Navy commander "as full of enthusiasm and adventure as a young man," who was "the subject of universal praise, especially by the army that saw and appreciated the gallantry of his conduct, and its important bearing on the campaign." See Hoppin, *Life of Andrew Hull Foote*, 390.



Boy on the Bridge: The Story of John Shalikashvili's American Success

By Andrew Marble

University Press of Kentucky, 2019
416 pp. \$36.95

ISBN: 978-0813178028

Reviewed by Bryon Greenwald

Biographies are frequently hit or miss and often tell linear, one-dimensional stories. The value of a biography as a contribution to a larger history depends on how broad an intellectual swath the author cuts and how extensive and probing the research. The wider the cut, the greater the chance the reader will learn not only about the subject but also about the greater social, cultural, political, and technological aspects of the subject's lifetime. The deeper the research, the more one learns both about the subject and the key events during his or her career. *Boy on the Bridge: The Story of John Shalikashvili's American Success*, Andrew Marble's thoroughly researched and exquisitely crafted biography of former Army general and Chairman of the Joint Chiefs of Staff John Shalikashvili, is an excellent example of a biography

that tells a compelling story and offers the reader a window into the surprising life of an American success story.

As Marble highlights, General Shali, as he preferred to be called, was a reserved, self-effacing consensus-builder who liked to avoid conflict and enjoyed giving others credit for actions he clearly set in motion. He shied away from publicity, albeit while making history. He twice told Secretary of Defense Les Aspin and President Bill Clinton that he did not want to be the Chairman of the Joint Chiefs of Staff. Shali was not the sort of man nor had the type of military career that normally produces great biography. After Colin Powell, few Chairman have risen to any level of historical prominence. Still, from the opening pages of *Boy on the Bridge*, the reader will be surprised by Shali's life and all he achieved. Indeed, his life reflects the intermingling of society, culture, and war that was so prevalent in the 20th century.

His maternal grandfather served in the high command of Russia's Tsar Nicholas II. His father, Dimitri, fought in World War I on the Russian side but returned to Georgia after the Bolshevik Revolution. After the war, Dimitri moved to Poland, where he married Shali's mother, Maria "Missy" Rudiger. When Germany attacked Poland in September 1939, Dimitri fought with the Poles, and in a twist of geopolitics, served at the end of the war as a member of the Georgian Legion supporting the Germans in Normandy and Italy before ending the war supporting Italian partisans against the communists in northern Italy. As a child, Shali witnessed the starvation and privation of Polish Jews in Warsaw before fleeing with his mother, brother, and sister to Germany to escape the oncoming Soviet Army. There, on April 24, 1945, in Pappenheim, Germany, 8-year-old John Shalikashvili met his first Americans, members of the 86th Infantry Division that had chased German SS troops out of the small town. In 1952, Shali immigrated to America and went to high school in Peoria, Illinois. He attended college and entered the Army through Officer Candidate School, served in the Artillery and Air Defense when it was a single branch, and then in the Artillery

for the rest of his career, including a tour in Vietnam.

As formative as those early years were, it was his service as a general officer that commands Shali to history. As the deputy commander of U.S. Army Europe in 1990, Shalikashvili was responsible for moving VII U.S. Corps from Germany to Saudi Arabia to provide General H. Norman Schwarzkopf with enough combat power to eject the Iraqi army from Kuwait, an immense multinational logistical undertaking. Immediately after the Persian Gulf War, Shali's greatest achievement came as the commander of Operation *Provide Comfort*, the 30,000-strong multinational relief effort to save 500,000 Kurds who had fled Iraqi forces into the high desert mountains and were dying by the thousands from harsh conditions, malnutrition, and disease. Shali organized forces from 13 countries and over 50 international and nongovernmental organizations to establish supply routes and basic infrastructure across an area of 83,000 square miles. Later, as Supreme Allied Commander, Europe, he traveled throughout Eastern Europe encouraging newly independent nations and calming Russian fears. Finally, as Chairman of the Joint Chiefs of Staff from 1993 to 1997, General Shali oversaw the deployment of forces to Somalia, Haiti, and Bosnia and provided a steady hand during the reduction in forces following the end of the Cold War. He died in 2011 from complications following a stroke.

Marble's fine biography offers much to the military reader. Beyond his significant accomplishments, General Shali is best known and remembered for his patience, empathy, and calm demeanor. In a world of Type A officers and leaders, he was a competent and capable Type B who treated everyone with dignity and respect, who set high standards and looked after those with whom he served, and who rose from extremely desperate beginnings to become the most senior man in the American military. JFQ

Dr. Bryon Greenwald is a Professor of History in the Joint Advanced Warfighting School, Joint Forces Staff College, at the National Defense University.

To Build a Better World

CHOICES TO END THE COLD WAR AND CREATE A GLOBAL COMMONWEALTH

Philip Zelikow & Condoleezza Rice



To Build a Better World: Choices to End the Cold War and Create a Global Commonwealth

By Philip Zelikow and Condoleezza Rice

Twelve, 2019

528 pp. \$22.99

ISBN: 978-1538764671

Reviewed by Walter M. Hudson

Philip Zelikow and Condoleezza Rice's *To Build a Better World* begins in early 1989, with two nobodies: one, a dutiful KGB officer in Dresden; the other, a research scientist at the East German Central Institute of Physical Chemistry. Like the rest of the world, they do not know what will take place through the course of that pivotal year, or how the aftermath will one day lead these two unknowns, Vladimir Putin and Angela Merkel, to the pinnacle of power.

It is a fitting introduction; how little do we really know about how events will unfold? The so-called experts certainly did not have it right. Well into the late 1980s, the accepted thinking among the intelligentsia was that the Cold War would continue into the foreseeable future and that the "American Century" was ending.

Then, in the blink of an eye, the Cold War ended and the Soviet Union ceased to exist. Talk of America's decline was consigned to history's ash heap and the American Century appeared unassailable. Things are hardly so sanguine now. Nonetheless, the end of the Cold War—with the free market system and the democratic order vindicated—still seems something a little short of miraculous. But perhaps it was not so. Human agency decisively intervened at every point. The end, as the authors make explicit in the book's subtitle, was determined by *choices* made. Zelikow and Rice's "analytical history of the major choices" zooms in on human beings and the choices they made during one of the 20th century's great pivot points.

Zelikow and Rice have done a very fine, scholarly job. Of course, they write not only as scholars but also as actors who played parts in that history. This opens them up to some criticism—how can they be objective? They are, however, forthright about it and occasionally place themselves in the narrative, a seeming overt acknowledgment of this sort of participant history. And it is familiar scholarly territory for them, both having previously navigated this subject matter in their *Germany Unified and Europe Transformed: A Study in Statecraft* (Harvard University Press, 1995). That was a good study, but still a case of near-first impression. Deeper scholarship, more declassification, and the passage of time provide for greater context and make the current title a much richer work.

Zelikow and Rice demonstrate impressive multiarchival, primary source research in a variety of languages to buttress their insights. This scholarship makes it a worthy addition to the growing body of literature examining the end of the Cold War, and, at a minimum, their book supplements traditional Cold War histories, such as the recent magisterial work of Odd Arne Westad, and earlier works by Cold War deans John Lewis Gaddis and Melvyn Leffler.

The book is also highly accessible and offers carefully sketched portraits of key world leaders grappling with the

decisions of their time. The portrait of Mikhail Gorbachev is sympathetic yet ultimately unflattering. George H.W. Bush and Helmut Kohl, on the other hand, are highlighted as capable stewards and leaders, and, in Kohl's case, the German chancellor is portrayed as a near-visionary statesman.

However, Zelikow and Rice do not only offer interesting character studies; the book is more fundamentally about strategic choices and the strategy of decisionmaking. Too often, histories that focus on so-called grand strategy appear as roadmaps to preordained destinations. The "blindness of hindsight," as Zelikow and Rice observe, is powerful. Retrospection confers a sense of the inevitable on events. Historians discern patterns in policymakers' decisions that operate in accordance with Alexander George's famous phrase, "operational codes." To do strategy is to have a mapped out "plan." In senior Service college terms, having a strategy is to have determined "ends, ways, and means."

But strategy is not simply planning; it is *doing*, which means strategist-statesmen are constantly *choosing* what to do. A strategy is often far less a set of rock-solid propositions that become long-range goals and more a series of tentative questions that require immediate answers. Zelikow and Rice's excellent work offers a thorough appreciation of strategy as choice-making.

In order to unpack how strategic choices are made, they rely on "Vickers Triangle," a formulation composed by the brilliant British polymath Geoffrey Vickers. This triangle is composed of values (what one cares about), realities (what the facts are), and actions (what one can actually do). Values, realities, and actions, as opposed to ends, ways, and means, are not linear; they are, in a Clausewitzian sense, relational. They constantly react and interact with each other to create new issues, new questions, and new understandings. They form a crucible from which judgments and choices, framed and reframed, are made in the urgency of the moment.

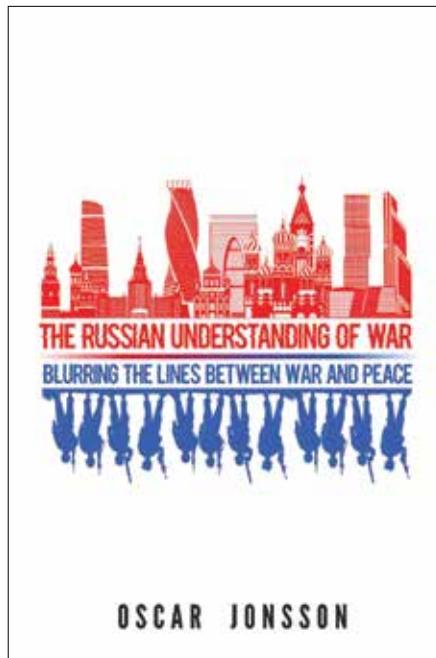
Thus, Zelikow and Rice frequently break *in medias res* and present "issue

maps” that pose a large geopolitical strategic issue, such as “Ending the Cold War in Europe.” Below that issue, the authors posit broad themes such as “Security in Europe.” They then pose a series of questions that lead to choices such as “Should the U.S. keep troops in Europe or not?”

Such questions, sifted through the interaction of values, realities, and actions, had to be answered. Choices *had* to be made. This is what strategy formulation was during the end of the Cold War. Indeed, one could argue that this is what strategy always is: fork-in-the-road decisions made with incomplete and sometimes confusing data. Some leaders, such as Gorbachev, made decisions that tended to be more wrong than right; others, such as Bush and Kohl, made ones that tended to be more right than wrong. For policymakers, warfighters, and students of strategy throughout the joint force, the insights offered should be of immediate value.

The Cold War ended three decades ago. For a brief moment, history itself appeared to have ended in a way that signaled the ascent of American ideals worldwide, in perpetuity. That moment has passed, no doubt. Nonetheless, as Zelikow and Rice point out, we would do well to remember our triumphs as well as our defeats, and recall that both result from deliberate choices and not simply historical accidents. JFQ

Colonel Walter M. Hudson, USA, is an Assistant Professor and Deputy Chair of National Security and Economic Policy in the Eisenhower School of National Security and Resource Strategy at the National Defense University in Washington, DC.



The Russian Understanding of War: Blurring the Lines Between War and Peace

By Oscar Jonsson

Georgetown University Press, 2019

208 pp. \$98.95

ISBN: 978-162617339

Reviewed by Mariya Y. Omelicheva

If you know the enemy and know yourself, you need not fear the result of a hundred battles,” wrote the influential Chinese military strategist Sun Tzu in *The Art of War*. Russia’s ongoing efforts to reshape the world in ways that are at odds with American values and interests have turned Moscow into a dangerous adversary. Countless analyses have appeared in recent years that venture to understand how Russian leadership thinks, what Russia wants, and how it plans to get it. Oscar Jonsson’s *The Russian Understanding of War* is a valuable addition to the corpus of knowledge on Russia’s military thinking about war.

Relying on a close reading of Russian security, military, and foreign policy doctrines and the writings of Russian military, academic, and political elites, Jonsson traces the evolution of Russian

military thought about war from the early Soviet period through contemporary times. According to Jonsson, the nature of war—traditionally understood in Russia as armed violence for political purposes—had not changed much until recently. The advent of information-psychological warfare has led to the blurring of the boundary between war and peace. Having observed the role of information in “altering the consciousness of a country” and undermining public trust in state institutions “to the degree that citizens are prepared to revolt, creating color revolutions,” Russian strategists began conceiving of information as a weapon and a more effective means of achieving strategic outcomes than armed force.

The surge of interest in Russia’s thinking stems from the growing awareness that Western strategic and military concepts may have limited utility for deciphering Russia’s purposes, perspectives, and mental models on war. Notwithstanding an appreciation of the fundamental differences in countries’ conceptions of war, Jonsson chooses to approach Russia’s views on armed conflict from a longstanding Western military theoretical background informed by a Clausewitzian perspective, rather than alternative “lenses” grounded in Russia’s own military theory. By doing so, the author falls into the same trap of ascertaining the seemingly novel Russian approach to operations for a fundamentally new conception of war, as many other writers on hybrid warfare and the Gerasimov doctrine have been caught in before.

Russia’s information-psychological operations are anything but new. They repurpose tried-and-tested malign influence campaigns used by the Soviets in Eastern and Western Europe. Similar to modern Russian strategists, the Soviet military and political elite recognized the economic and technological superiority of the United States and sought to compensate for capability gaps by exploiting cultural values and psychological biases in individual decisionmaking processes. Questions about the nature versus the character of war were not at the forefront of Soviet thinking, which,

as Jonsson aptly discusses in his book, was highly ideologized and focused on issues of just war versus unjust war. The Soviet holistic approach to war, which treated armed conflict as a complex sociopolitical phenomenon and part of a single synthetic system, stands in stark contrast to Western and American analytical perspectives. Soviet military thinkers envisioned the enemy as a system, and the operational logic that built on this approach required neutralizing the enemy's ability to attain its goals. Information-psychological operations were instrumental and remain ingrained in modern Russian military thinking.

The key premise of the book, however, remains timely and valid. Knowing one's opponent is the first step to developing effective countermeasures. The core argument of Jonsson's study emphasizes the fact that Russia has conceptualized war as a continuation of politics, and politics as a continuation of war, thus rendering the binary "peace or war" paradigm of the operational environment obsolete. Many joint force operational and strategic concepts are developed wholly or in part on the assumption of operations taking place in either a distinct state of peace or war. The Joint Operating Environment 2035 envisions challenges that are significantly different from those of recent decades. One of the main challenges—the contest over ideas and norms—will take place entirely in the information domain. Jonsson's volume speaks directly to the joint force concepts for operating in the information environment by reminding us that Russia has conceptualized information holistically, embracing not only the technological aspects of information but also its psychological aspects. U.S. and Western approaches to information tend to be more technologically biased and infrastructure-centered, not sufficiently integrating less tangible (cognitive and perceptual) methods of manipulation.

To truly understand an adversary requires delving deeper into its politics, culture, and society. While a valuable guide to Russia's thinking about war, Jonsson's book should be read in

conjunction with other studies in Russia's decisionmaking, such as Marlène Laruelle and Jean Radvanyi, *Understanding Russia: The Challenge of Transformation* (Rowman and Littlefield, 2018); Bettina Renz, *Russia's Military Revival* (Polity, 2018); Roger E. Kanet, ed., *Routledge Handbook of Russian Security* (Routledge, 2019). These works offer a comprehensive collection of chapters on all aspects of Russian security and foreign policy.

Although an authoritarian regime, the Kremlin is captive to opaque and intricate inner power struggles and attentive to public sentiments. These domestic considerations can either amplify or lower the threshold for the use of force and the acceptance of risk, thus affecting the use of information operations. It is also vital to recognize that Russian policymakers and strategists perceive the world through mirror images. The Kremlin ideologues are convinced that the West uses similar, if not the same, concepts and methods of information war against them. Therefore, it is not that Russian conduct always follows Russian theorizing about war, but Russian theorizing about war can be used to justify Russia's own conduct and criticize the West. Lastly, the emphasis on understanding Russia's information warfare should not blind us to Russia's readiness to use military force.

The Russian Understanding of War is a useful read for all national security analysts and strategists, as well as Russia-watchers throughout the joint force. Ultimately, Jonsson succeeds in his goal of providing a helpful guide to understanding an adversary that has embraced a form of conflict at odds with Western notions of war and peace. JFQ

Dr. Mariya Y. Omelicheva is a Professor of Strategy at the National War College at the National Defense University in Washington, DC.

New from NDU Press

for the Center for Strategic Research

Strategic Forum 302

The European Union's Permanent Structured Cooperation: Implications for Transatlantic Security

By Jonathan Dunn



Many U.S. defense officials expressed concern over the EU's November 2017 launch of its Permanent Structured Cooperation. They fear that a more capable EU would make it a competitor to NATO for European security issues, and in so doing reduce U.S. influence in European security. Concerns about diminished U.S. influence and EU divergence from NATO as a result of PESCO are misguided. Rather than be concerned about the remote possibility of European strategic autonomy, the United States should throw its full support behind the PESCO initiative and other attempts to strengthen European defense. That said, the United States has an interest in the direction that the EU takes with PESCO and should therefore attempt to shape it constructively.



Visit the NDU Press Web site for more information on publications at ndupress.ndu.edu



F/A-18F Super Hornet assigned to "Diamondbacks" of Strike Fighter Squadron, attached to Carrier Air Wing 5102, conducts flight operations, Atsugi, Japan, January 29, 2020 (U.S. Navy/Alex Grammar)

Airbase Defense Falls Between the Cracks

By Joseph T. Buontempo and Joseph E. Ringer

The fielding of fifth-generation aircraft like the F-22 and F-35 underscores the U.S. Air Force's ability to contribute to national-level objectives by refocusing on threats posed by surging strategic competitors such as Russia and China. These latest generation aircraft are primed to continue America's dominance in the air. But what happens when they are on the ground? On an airbase, the latest in stealth aircraft technology is not likely to cloak these aircraft from forces seeking an asymmetric advantage to

counter Air Force superiority. The survivability of these assets is paramount to mission success. Furthermore, unlike the setbacks stemming from attacks on airbases in past wars, when aircraft replaceability played a muted role in basing considerations, today's jets, with unit costs of \$100 million or more, considerably escalate the consequences of failing to secure the airbase from attacks. These economic considerations are now a factor for beddown of any fifth-generation aircraft during combat operations, with replaceability also

assuming a prominent role in basing deliberations. For all their advanced technology, aeronautical superiority, and advanced situational awareness capabilities, fifth-generation aircraft share a feature with the Curtiss P-1 Hawk of the 1920s: they are vulnerable while on the ground.

Over the last few decades, locating U.S. overseas airbases far from the enemy has been sufficient to protect them during large-scale military operations. With the return of better organized, trained, and technologically equipped near-peers, however, distance is unlikely to provide refuge from the long reach of these more capable adversaries. This article considers two types of threats that could pose a serious challenge to airbases in the near future. The first is direct and indirect attacks to rear-area operations by adversary special operators, and the second is theater ballistic and cruise missile attacks. The Department of Defense (DOD) places responsibility for protecting airbases against such threats with the Air Force and Army (and host-nation forces as applicable). Unfortunately, airbase defense can fall between the cracks. The resulting

Dr. Joseph T. Buontempo is Assistant Director of the System Evaluation Division at the Institute for Defense Analyses. Lieutenant Colonel Joseph E. Ringer, USAF, is Senior Program Evaluator in Investigative Oversight and Special Investigations and Review at the Department of Defense Office of Inspector General.

deficit, which is likely to continue long into the future, can result in significant gaps in the defense of airbases.

Defense Against Special Operators

Highly trained and well-equipped special operators and extensive agent and sleeper cell networks, whose mission is to engage the fixed locations where airbase operations occur, present an acute threat to U.S. air operations. History provides many case studies on the devastating effect ground attacks can have on air operations. For insight on what this shift could mean to base defense, the Air Force needs to look no further than the Vietnam War, where roughly 1,600 aircraft were damaged or destroyed by Vietcong and North Vietnamese rocket and mortar attacks.¹ Likewise, the efficacy of British Special Air Services attacks on Axis airfields across North Africa during World War II, destroying 367 aircraft plus support facilities and equipment,² should remind airbase planners of the destructive precision of highly trained special operators and the ineffectiveness of distance as a means for security. Undoubtedly, today's advances in weapons, such as GPS-guided mortars, small unmanned aerial systems, and large-caliber sniper rifles, will serve to enhance the effectiveness and lethality of these elite forces. While true worldwide, it is particularly acute on the Korean Peninsula where it is estimated that North Korea employs nearly 200,000 special operations forces specifically trained to establish a second front, conduct sabotage operations, and attack high-value targets such as command and control nodes and airbases in South Korea.³

In many ways, the limited number of attacks on airbases experienced in recent wars and insurgencies has stunted U.S. development of airbase defense concepts and schemes to counter the capabilities of highly trained special operators. Moreover, the recently observed ineffectiveness of insurgents' use of standoff weapons, which should not be confused with the lethal precision with which advanced special operators employ

the same weapon systems, may have served to further downplay the threat. But as the Air Force looks to grow its operational squadrons by 25 percent, base defense planners must reassess the impact this increase in beddown requirements will have on base defense forces and resources within a risk-based framework. The risk presented by threats such as special operations forces, irregular forces, and small tactical units, particularly from standoff weapons, is widely known yet insufficiently addressed. Given the history of conflict, particularly during the latter half of the 20th century, when standoff weapons attacks proved to be particularly effective in damaging and destroying aircraft,⁴ effective controls and countermeasures to manage the risk posed by this threat are crucial for fielding fifth-generation aircraft. The emergence of small unmanned aerial systems as a threat to airbase operations adds even more incentives.

Within joint operating areas, airbases are intended to be protected in layers and in depth. Typically, base security forces defend from the base boundary inward, and U.S. Army Air Defense Artillery units, when available, provide cover from attacks from the air. Mobile security forces and, as required, Army tactical combat forces or host-nation security forces provide external defense from the base boundary outward. However, with base security forces as the lone exception, none of the entities responsible for security outside the base boundary are under the operational or tactical control of the airbase commander. This particularly consequential concern is made worse if the base boundary does not encompass the effective range of standoff weapons or if host-nation restrictions preclude U.S. forces from venturing "outside the wire." Thus, defense outside the base boundary is often subject to limited ground force availability and competing area commander or host-nation commander requirements. These demands, which can result in the absence of defending forces, may produce seams and gaps within the joint force's defense of airbases.

Events in recent conflicts have accentuated the potential for disastrous

consequences due to insufficient planning and resourcing for base defense and force protection. In the 2012 ground attack on Camp Bastion in Afghanistan, a team of 15 heavily armed and well-trained—but not to the level of special forces—Taliban insurgents successfully infiltrated the base boundary and perimeter defenses to destroy six Marine Harrier aircraft with antipersonnel grenades. They also damaged ten other aircraft along with support facilities and assorted equipment.⁵ Furthermore, 2 friendly forces were killed and 17 individuals wounded.⁶ A subsequent U.S. Army investigation into the attack cited "failure to ensure that an integrated, layered, defense-in-depth was in place" as the causal factor for this base defense failure.⁷ It also listed underestimation of the enemy, lack of unity of command for security, and failure to manage risk and vulnerabilities as contributing factors.⁸ Airbase commanders faced a similar dilemma in Vietnam, where base defense was not viewed as a high priority for resources by higher echelons of command and, as a result, remained vulnerable to ground attack throughout the war.⁹

Joint doctrine recognizes the increased vulnerability of aircraft to attacks staged from areas contiguous to airbases during takeoff and landings, as well as when parked.¹⁰ It even highlights the need to coordinate with area commanders to ensure base boundaries are adjusted to provide adequate protection from rocket, artillery, and mortar attacks. But joint doctrine stops short of prescribing inclusion of the effective ranges of these indirect fire weapons, also referred to as a "footprint," within the airbase boundary.¹¹ Yet, to be effective, the base defense plan must include key terrain outside the base boundary from which the enemy could affect air and space operations, in addition to the area inside the base boundary.

Guided by the principle that air and space assets are most vulnerable on the ground, Air Force Security Forces protect the base from the boundary inward by conducting operations to deter, delay, and defeat threats ranging from agents, partisans, and terrorists to small tactical

units and special operations forces.¹² Using an Integrated Defense concept to meld various Air Force capabilities into a comprehensive base defense strategy, base defense planners seek to leverage assigned resources against adaptive threats to protect U.S. and coalition missions and personnel. However, the Air Force's base defense inventory does not include organic counter-rocket, -artillery, and -mortar capabilities or the associated threat early warning alert systems. This capability must be coordinated with the Army or host-nation forces, if available.¹³ While joint doctrine does not assign responsibility for counter-indirect fire to any Service component specifically, U.S. Army considers the ability to attack and defeat enemy rocket, artillery, and mortar attacks to be an air and missile defense competency that is executed by the Army within authorities granted by the joint force air component commander.¹⁴ Undoubtedly the Army's capacity to support airbases with counter-indirect fire systems and associated threat early warning alert systems will be further stressed by the Air Force's force structure expansion plans and emerging concepts for distributed operations.

To account for the standoff range of indirect fire weapons, Air Force base defense planners developed the base security zone (BSZ) concept. The BSZ is an Air Force–unique construct that considers the area outside the base boundary—from which standoff and indirect fire weapons can engage the base and aircraft on approach and departure—in base defense planning.¹⁵ After identifying the BSZ, the installation commander must then negotiate adjustment of this boundary to include those areas of concern that may extend far beyond the original base boundary.¹⁶ Conceptually, establishing the BSZ is intended to expand the installation commander's authority and ability to directly address ground-based threats to airfield operations. However, in practice, it is not quite that simple, as the battlespace outside the base boundary is defined and controlled by the Army or host-nation forces, and approval from the area or host-nation commander is

required before the base boundary can be adjusted to account for standoff threats.

Within the BSZ, efforts of security forces, or other base defense forces assigned area security duties, to suppress indirect fire threats consist of physical presence, aggressive patrolling, and limited active defensive measures designed to deny adversaries access to the standoff footprint.¹⁷ Intriguingly, however, in what amounts to a significant omission for joint security operations planning, the BSZ is recognized as a planning construct that is used only by the air component.¹⁸

Defense Against Ballistic and Cruise Missiles

Russia and China continue to develop ballistic and cruise missiles with increasing accuracy, range, and complexity, and in increasing numbers, which could present a significant threat to U.S. forces in theater.¹⁹ Currently, China has robust capabilities against bases and facilities extending to the First Island Chain in the Pacific Ocean, is acquiring an increasing number of medium-range ballistic missiles and cruise missiles that could hold at risk U.S. bases in Japan, and is looking to expand its capabilities to attack targets throughout the western Pacific Ocean, including U.S. bases and facilities on Guam.²⁰ Although its long-range strike capabilities currently have limitations, “China’s commitment to continuing to modernize its strike capabilities indicates the risk will likely grow going forward.”²¹

Russia has made a priority of developing cruise and ballistic missiles in the 21st century.²² In particular, Russia has made “significant progress over the last decade operationalizing its long-range precision-strike capabilities, which could pose a significant threat to U.S. and NATO [North Atlantic Treaty Organization] bases, ships, and other military and civilian infrastructure targets in the European theater.”²³ Notably, since 2014, the United States has found Russia to be in violation of the 1987 Intermediate-Range Nuclear Forces Treaty by developing and deploying a ground-launched cruise missile with a range of 500 kilometers (km) to 5,500 km, which would

potentially enable it to reach targets in most of NATO’s European countries.²⁴ Alarmingly, both Russia and China are also developing maneuverable hypersonic glide vehicles, which can glide at Mach 5 or greater at low altitudes.²⁵

Russia or China could use ballistic and cruise missiles to target U.S. airbases to make the task of generating sorties difficult. RAND has examined the potential effects of Chinese ballistic and cruise missiles on U.S. airbases in the Pacific.²⁶ They found that approximately 30 to 50 ballistic missiles targeting an airbase could destroy air defenses and aircraft parked in all open parking areas and crater runways to prevent launching and recovering aircraft. In addition, if China simultaneously launched another 30 to 50 cruise missiles against the same airbase, they could also damage or destroy aircraft shelters, as well as fuel, maintenance, and other facilities. Based on its analysis in a combat scenario, RAND concluded that, by comparing the numbers of missiles needed “to close bases with the numbers that China is currently fielding, clearly the United States could face extended periods of time where few, if any, of our bases near China are operating.”²⁷

Countering air and missile threats to protect airbases and other critical assets is described in Joint Publication 3-01. At the theater level, the counterair mission “is the foundational framework”²⁸ for countering air and missile threats and “is inherently a joint and interdependent endeavor.”²⁹ It consists of defensive counterair (DCA) operations supported by offensive counterair (OCA) attack operations. DCA operations consist of both active defenses, which engage and attempt to destroy attacking aircraft and missiles, and passive defenses, which include all the other measures used to reduce the effectiveness of the threats.³⁰ Some of the major active defense weapons systems include the Air Force surveillance and fighter aircraft, U.S. Army Patriot defense systems, U.S. Navy Aegis ships and Standard Missile interceptors, and Terminal High Altitude Area Defense (THAAD) systems. Passive defenses include detection and warning systems; camouflage, concealment, and



Senior Airman, response force leader with 791st Missile Security Forces Squadron, performs security sweep of landing zone near Minot Air Force Base, North Dakota, on January 25, 2017 (U.S. Air Force/Brandon Shapiro)

deception; dispersal of assets; and hardening of structures. If the United States is unable to conduct attack operations prior to threats being launched, “DCA, which is by nature reactive, must be flexible enough to prevent the enemy from gaining the initiative.”³¹

Although a comprehensive doctrine exists for countering air and missile threats, in practice the Services can struggle to follow this doctrine. For instance, not only are a fixed number of U.S. Air Force fighter aircraft needed for both DCA and OCA attack operations, they are also needed for three other OCA operations—suppression of enemy air defenses, fighter escort, and fighter sweep—and also to support other missions, including strategic attack, air interdiction, and close air support.³² Compounding this problem are the challenges the Air Force is facing in maintaining the readiness of its fleet of aircraft,

due in part to the significant deployment rates experienced over the last couple of decades and to shortfalls in the numbers of pilots and aircraft maintainers.³³ For example, the 2017 mission-capable rates are approximately 49 percent for the F-22A, 55 percent for the F-35A, and 70 to 75 percent for the F-15 variants.³⁴

The United States also does not have enough Army air and missile defense systems to protect every critical asset or enough interceptors to engage large threat salvos. Although DOD has invested in these capabilities, it “still lacks the ability to defeat large numbers of ballistic missiles, cruise missiles, unmanned aircraft, and other emerging guided weapons threats.”³⁵ Patriot systems, for instance, “are expensive and their combined capacity would be insufficient to protect airbases and other military infrastructure that U.S. and allied forces would depend on during a major conflict with a great

power.”³⁶ Although the Army continues to invest in improving its capabilities to defeat ballistic and cruise missiles, this spending must also be used for programs, such as the Stryker-based Initial Maneuver Short-Range Air Defense system,³⁷ intended to protect maneuver forces. THAAD and some Navy Aegis ships can help provide protection against ballistic missiles if they are positioned to do so. However, as former Chief of Naval Operations Admiral Jonathan Greenert and former Army Chief of Staff General Raymond Odierno recently emphasized, there are “growing challenges associated with ballistic missile threats that are increasingly capable, continue to outpace our active defense systems, and exceed our Services’ capacity to meet Combatant Commanders’ demand.”³⁸

Even when they are available to defend airbases and other critical assets, active defense systems can have

performance limitations against advanced threats that reduce their effectiveness against these threats. To illustrate, a ballistic missile can challenge missile defense systems by following a depressed trajectory or releasing a maneuvering warhead or can carry penetration aids that attempt “to deceive, obscure, or jam sensors used to detect and track missiles and [reentry vehicles].”³⁹ Likewise, cruise missiles can attempt to hide from air defense radars by flying at low altitude or behind terrain features or by incorporating stealth design features.⁴⁰ In addition, salvos of ballistic and cruise missiles can be launched in a way to simultaneously strike an airbase in an attempt to overwhelm the raid handling capabilities of defensive systems. Finally, as stated above, Russia and China are developing hypersonic glide vehicles, and the “combination of high speed, maneuverability, and relatively low altitude makes them challenging targets for missile defense systems.”⁴¹

The challenges associated with active defense make difficult the task of protecting airbases from air and missile threats. Moreover, because of the luxury of being able to use distance to help provide protection over the last few decades, passive defense measures have received short shrift for airbase defense. Although this situation could likely be improved, the seam between Air Force and Army responsibilities for providing air and missile protection allows each Service to implicitly assume that the other will fill any gaps, resulting in persistent limitations in protection.

The Way Forward

To better prepare for the reemergence of highly capable nation-state actors, joint effort is needed to reduce the number of seams in airbase defense and to close gaps where possible to help ensure the availability of airpower within a contested environment. One solution is to include the BSZ in joint doctrine as a construct for joint security operations planning as opposed to merely a tool used by air component planners. Currently, joint doctrine recognizes the threat posed by standoff

weapons in areas contiguous to airbases and suggests the base boundary should be adjusted to account for these threats. It also recognizes the BSZ, but only as an air component planning construct. But these two points represent the issue; if it remains a suggestion, or something that should happen in air component planning, the default starting point for airbase defense planning remains status quo at best, and a point of contention at worst. Current joint guidance discusses what should be done, but the BSZ construct represents how it ought to be done to maximize effectiveness—succinctly and without ambiguity—from an air-minded perspective.

Codifying the BSZ as a joint security operations planning construct and battlespace, and identifying the installation commander as the battlespace owner, would eliminate the need to negotiate adjustments to the base boundary to account for the effective range of indirect fire threats. This would save time and potentially eliminate confusion related to boundary and area adjustments. Service components would need to assess the impact of such a decision, since one potential outcome is an increase in the demand for base security forces and resources. The BSZ concept also would facilitate deliberations about who defends what and to what extent, as seen through the eyes of the battlespace owner—an Airman. A battlespace that includes standoff threats, previously the responsibility of the commander of the joint security area, would now be under the authority of the airbase commander. This is not intended to imply the joint force commanders’ authority to make force and resource allocation decisions, above the base and area security commanders’ level, should be changed; rather, the joint force commanders’ decisions regarding the shape of, and assets assigned to, the BSZ would influence which aircraft operated from a given location within a greater risk-management framework.

The complex nature of the environments where the Air Force may be tasked to operate, combined with the availability of joint and host-nation support, will undoubtedly necessitate some adjustments

to the BSZ. But by establishing the BSZ as a battlespace within the joint operating area, a premise that considers threats to air operations across multiple domains will be formalized for use during campaign, deliberate, and crisis action planning for joint operations.

In addition, the Air Force should formally adopt a risk-based planning strategy for establishing airbases. This approach would explicitly account for defenses against the spectrum of likely threats as a critical planning factor. In doing so, the Air Force would address the multiple tradeoffs needed to effectively execute its mission while protecting its airbases. For example, an airbase could be located beyond the reach of relevant threats, but this might require strike aircraft to travel longer distances, resulting in less time spent on station, reduced sortie generation rates, and the procurement of additional tanker support. Risk-based airbase planning would also incentivize planners to adopt, wherever possible, methods to reduce the dangers posed by such threats. Passive defenses, in particular, are likely to play a significant role. Perhaps most important, airbase threat detection and warning systems could enable Airmen to adequately take cover when necessary. Other passive measures include camouflage, concealment, and deception; dispersal of on-base assets; and hardening of structures. Likewise, expeditionary basing and dispersed basing might help protect bases by making them more difficult for the enemy to monitor, target, and attack. However, this is not without its own set of base defense challenges. Multiple and likely smaller bases might not be capable of supporting the infrastructure available on permanent bases. Also, using many bases requires more forces and resources for protection and defense. In fact, given force structure limitations, it is doubtful that the Army or host-nation equivalent will be able to support simultaneous base defense tasks across a theater.

The planning process described above—not to be confused with the risk-based model the Air Force currently uses for Integrated Defense—would support deliberate and crisis action planning



Army test-fires Patriot missile, March 27, 2019 (U.S. Army/Jason Cutshaw)

in determining where assets should be based and what level of security will be assigned to each location. Under the most desirable conditions, sites capable of supporting the BSZ construct under the command of one commander, without constraints imposed by the host nation or geographical features, would be assigned organic base defense forces to defend and patrol the entirety of the BSZ. Air defense assets could also be assigned to provide cover from theater missile threats. In particular, these assets could be used to protect capabilities not protected by passive measures. The comprehensive defensive scheme of these locations would present a reduced risk from ground and missile threats, and consequently could serve as the beddown locations for high-demand, low-density assets such as fifth-generation aircraft. Conversely, locations that could not support these base defense considerations could be considered for basing aircraft that are

easier to replace or have a smaller role in the overall campaign strategy. The result is a tiered and scalable assessment of potential airbases. This assessment, based on available and fixed vulnerability mitigating measures, would enable risk-based decisions regarding aircraft beddown in support of theater operations.

Conclusion

Joint, Air Force, and Army doctrine on airbase defense converge to form a complex system of systems. But the merge points of these concepts create seams and gaps that are ripe for exploitation by countries such as China, Russia, Iran, and North Korea. Considering America's technological advantage in the air, asymmetric attacks intended to disrupt and harass air operations on the ground remain a prudent and likely course of action for these nation-states.

One prominent seam occurs at the interface of the base boundary and the

area immediately outside of the boundary, where area security operations occur. Two forces, Soldiers and Airmen, under two different commands in two separate areas of responsibility, conduct defensive operations near one another in order to deny access to the base and deter use of standoff weapons. Though battlefield co-ordination processes that are designed to protect critical resources and reduce the likelihood of fratricide appear throughout joint doctrine, the complexity and sheer number of these processes give rise to opportunities for miscommunication, misunderstandings, and divergent priorities. The latter case yields particularly dire consequences. Another prominent seam occurs in air and missile defense. Joint doctrine indicates that airbases will be protected by Air Force DCA operations and Army active defense systems. In practice, however, one Service implicitly assumes that the other will fill any gaps in defenses, resulting in limited protection.

The return of near-peer adversaries necessitates that the Air Force analyze all threats to airbases—the points of origin for all Air Force sorties flown. The formal adaptation of a risk-based airbase planning strategy will put the Air Force in a stronger position to decide the best courses of action for protecting airbases while executing its missions, and to decide how to judiciously employ the limited defense capabilities that the Army and host nations might bring. Central to this strategy is formalizing the BSZ as a planning construct for joint security operations. By examining all the relevant threats, tradeoffs, and mitigation measures pertaining to the BSZ, the Air Force would also be better postured to advocate for additional passive, active, and nonkinetic defenses, in terms of both procuring additional systems and developing new systems. The Air Force, then, must examine the tradeoffs between executing its missions and fully protecting its airbases in a manner similar to that used by the Navy when planning for the deployment of its aircraft carriers. For, in both cases, all the advanced fighter aircraft technologies designed to defeat a highly capable adversary will be for naught if the aircraft are destroyed before takeoff, or if the surface-based operations are forced to leave the theater. JFQ

Notes

¹ Alan J. Vick, *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges* (Santa Monica, CA: RAND, 2015), xii.

² Alan J. Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases* (Santa Monica, CA: RAND, 1995), 56.

³ Anthony H. Cordesman, *Korean Special, Asymmetric, and Paramilitary Forces*, with Charles Ayers and Aaron Lin (Washington, DC: Center for Strategic and International Studies, August 9, 2016), available at <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160809_Korean_Special_Asymmetric_Paramilitary_Forces.pdf>.

⁴ Vick, *Snakes in the Eagle's Nest*, 94.

⁵ William B. Garrett and Thomas M. Murray, *Army Regulation (AR) 15-6 Investigation of the 14–15 September 2012 Attack on the Camp Bastion, Leatherneck, and Shorabak (BLS) Complex, Helmand Province, Afghanistan* (Fort

Bragg, NC: Headquarters U.S. Army Forces Command, August 19, 2013), 2.

⁶ Ibid.

⁷ Ibid., 20.

⁸ Ibid., 24, 25, 29.

⁹ Roger P. Fox, *Air Base Defense in the Republic of Vietnam: 1961–1973* (Washington, DC: Office of Air Force History, 1979), 27.

¹⁰ Joint Publication (JP) 3-10, *Joint Security Operations in Theater* (Washington, DC: The Joint Staff, July 25, 2019), I-7, IV-17.

¹¹ Ibid., IV-17.

¹² Air Force Handbook (AFH) 31-109, *Integrated Defense in Expeditionary Environments* (Washington, DC: Headquarters Department of the U.S. Air Force, May 1, 2013), 5–6; Air Force Policy Directive 31-1, *Integrated Defense* (Washington, DC: Headquarters Department of the U.S. Air Force, 2018), 2-3; JP 3-10, IV-18.

¹³ JP 3-10, IV-18.

¹⁴ Army Doctrine Reference Publication 3-09, *Fires* (Washington, DC: Headquarters Department of the Army, February 2013), 1, 4.

¹⁵ AFH 31-109, 19–20.

¹⁶ Annex 4-0, *Combat Support*, Curtis E. LeMay Center for Doctrine Development and Education, January 5, 2020, available at <wwwdoctrine.af.mil/Portals/61/documents/Annex_4-0/4-0-Annex-COMBAT-SUPPORT.pdf>; Annex 3-10, *Force Protection*, Curtis E. LeMay Center for Doctrine Development and Education, January 5, 2020, available at <wwwdoctrine.af.mil/Portals/61/documents/Annex_3-10/3-10-Annex-FORCE%20PROTECTION.pdf>.

¹⁷ Vick, *Snakes in the Eagle's Nest*, 87.

¹⁸ JP 3-10, III-18.

¹⁹ *Ballistic and Cruise Missile Threat* (Washington, DC: National Air and Space Intelligence Center, in collaboration with the Defense Intelligence Ballistic Missile Analysis Committee, June 2017), 2, 35, 38.

²⁰ *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018* (Washington, DC: Office of the Secretary of Defense, May 16, 2018), 59, 118.

²¹ Jordan Wilson, *China's Expanding Ability to Conduct Conventional Missile Strikes on Guam* (Washington, DC: U.S.-China Economic and Security Review Commission, May 10, 2016), 3.

²² *Russian Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017), 35, 78.

²³ Kathleen H. Hicks et al., *Evaluating Future U.S. Army Force Posture in Europe: Phase II Report* (Washington, DC: Center for Strategic and International Studies, June 2016), 35.

²⁴ Amy F. Woolf, *Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress*, R43832 (Washington, DC: Congressional Research Service, December 7, 2018), summary, 26.

²⁵ *Ballistic and Cruise Missile Threat*, 8.

²⁶ Jeff Hagen, *Potential Effects of Chinese Aerospace Capabilities on U.S. Air Force Operations* (Santa Monica, CA: RAND, May 20, 2010).

²⁷ Ibid., 3.

²⁸ JP 3-01, *Countering Air and Missile Threats* (Washington, DC: The Joint Staff, April 21, 2017), I-1.

²⁹ Ibid., I-4.

³⁰ Ibid., I-6 to I-7.

³¹ Ibid., V-3.

³² Ibid., I-6.

³³ Stephen Losey, "Fewer Planes Are Ready to Fly: Air Force Mission-Capable Rates Decline Amid Pilot Crisis," *Air Force Times*, March 5, 2018.

³⁴ Ibid.

³⁵ Carl Rehberg and Mark Gunzinger, *Air and Missile Defense at a Crossroads: New Concepts and Technologies to Defend America's Overseas Bases* (Washington, DC: Center for Strategic and Budgetary Assessments, 2018), 1.

³⁶ Ibid., 11.

³⁷ Ashley Tressel, "Army Readying for IM-SHORAD Production," *Inside Defense*, February 12, 2019.

³⁸ Jonathan W. Greenert and Raymond T. Odierno, "Memorandum for Secretary of Defense, Subject: Adjusting the Ballistic Missile Defense Strategy," November 5, 2014, available at <<https://news.usni.org/2015/03/19/document-army-navy-memo-on-need-for-ballistic-missile-defense-strategy>>.

³⁹ *Ballistic and Cruise Missile Threat*, 9.

⁴⁰ Ibid., 35.

⁴¹ Ibid., 8.



Dr. Valbona Zeneli, Marshall Center's professor of National Security Studies, talks about "Crime and Corruption," August 12, 2016, during Program on Countering Transnational Organized Crime (George C. Marshall European Center for Security Studies/Christine June)

Putting the “FIL” into “DIME”

Growing Joint Understanding of the Instruments of Power

By Cesar Augusto Rodriguez, Timothy Charles Walton, and Hyong Chu

Despite how long the DIME has been used for describing the instruments of national power, U.S. policymakers and strategists have long understood that there are many more instruments involved in national security policy development and implementation.

—JOINT DOCTRINE NOTE 1-18, *STRATEGY*

Major Cesar Augusto Rodriguez, USAF, is Chief of the Air Force Section Honduras, U.S. Military Group, U.S. Embassy Tegucigalpa. Major Timothy Charles Walton, USA, is an Effects Integrator in the Counter-Facilitation Task Force at the Defense Threat Reduction Agency. Lieutenant Commander Hyong Chu, USN, is Supplier Relations and Program Management Division Chief of the Strategic Acquisition Programs in Defense Logistics Agency Land and Maritime.

While the U.S. military tends to view the instruments of power (IOPs) strictly through the lens of the diplomatic, informa-

tional, military, and economic (DIME) framework, it is increasingly imperative to consider additional IOPs such as finance, intelligence, and law enforcement (FIL). The U.S. military focuses primarily on the kinetic employment of the military, prioritizing the big *M* to demonstrate power, destroy the enemy, and celebrate victory. This military-centric approach often neglects other IOPs, resulting in suboptimal use of resources, the creation of an echo chamber, and poor transitions to other organizations, agencies, and/or national governments. The emergence of a new strategic environment necessitates an orchestration of multiple instruments of power. As a result, it is perhaps time to transition from a DIME to DIME-FIL concept.

U.S. peer competitors, namely Russia and China, have already developed alternative concepts to leverage IOPs to compete below the threshold of conflict. For example, Russia conceptualizes political warfare using nonmilitary and above-military categories (political, network, economic, financial, intelligence, legal, cultural, propaganda, drug, and so forth), which are similar to the DIME-FIL IOPs while continuing to emphasize the military instrument.¹ As peer competitors develop such fluid and threshold-based gray zone concepts, the United States must adapt in order to compete in a changing threat environment. To succeed, commanders and their staffs will need to understand, select, and synchronize IOPs to ensure a whole-of-government and international approach to these problem sets.

Currently, doctrine and planning emphasize the DIME model.² The scant literature on IOPs mentions the addition of FIL, but the focus has been its application to combating terrorism. The first mention of FIL pertaining to the National Security Strategy was in 2003, in a document that called for defeating terrorism through the direct and indirect use of DIME-FIL IOPs.³ Subsequently, similar language appeared in the 2006 National Military Strategic Plan for the war on terror and focused on cooperation among U.S. agencies, coalitions,

and partners to “integrate all instruments of U.S. and partner national power . . . DIME-FIL.”⁴

U.S. strategic direction and joint doctrine state the importance of synchronizing and incorporating a whole-of-government approach in order to utilize all IOPs for unity of effort. The Joint Force 2020 concept of globally integrated operations argues for a transregional, all-domain, and multifunctional approach and urges the joint force to prepare for the future competitive security environment by leveraging Service capabilities.⁵ However, this approach ignores the necessity of incorporating interagency and global partners and capabilities. Thus, a more strategic global integration concept is vital in today’s environment. *Global integration* is defined by Chairman of the Joint Chiefs of Staff Instruction 3100.01D and the *Summary of the 2018 National Defense Strategy of the United States of America* as “the arrangement of cohesive joint force actions in time, space, and purpose, executed as a whole to address transregional, multifunctional challenges across all domains through the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement and military.”⁶ The concept addresses the importance of a unified effort across all elements of national power and could provide a framework to incorporate global integration for the commander and planners to truly leverage all government agencies’ strengths, achieve military objectives, and ultimately protect national interests.

However, there is little explicit information on the new IOPs and even less guidance regarding the potential application of a more granular conception of IOPs in a competitive environment. Failing to clarify or ignoring the DIME-FIL concept leads to a lack of synchronization and global integration in the whole-of-government approach. Therefore, U.S. military leadership should consider adding the FIL IOPs to the DIME construct and incorporating it into joint doctrine to improve interorganizational planning for an international and intergovernmental approach in

the new environment of Great Power competition.

Clarifying the definition of FIL IOPs, identifying key mission partners, and detecting potential applications for each of the new FIL instruments can mitigate the gap in doctrine and planning. An increased understanding of the FIL IOPs will allow the U.S. military to update doctrine, synchronize the IOPs, become more globally integrated, and perform in the competitive environment, ultimately achieving unity of effort and effectively protecting national interests.

Understanding the FIL Instruments

Financial. The financial IOP was born during the war on terror, as the United States sought to disrupt and dismantle global terrorist financial networks. The National Security Strategy for Combating Terrorism identified the importance of affecting financial systems used by terrorist organizations that support their survival and continued operations.⁷ In relation to violent extremist organizations (VEOs), the financial IOP is characterized as the specific means by which insurgents acquire and distribute capital, whether via formal or informal banking and monetary exchange systems.⁸ The routine use, success, and precision of the financial IOP over the past two decades prove that it is an essential addition to DIME. Although the focus of the financial IOP has been on the VEO threat, it could be expanded to address other threats and actors including transnational crime organizations, state proxy groups, nonstate actors, and states. Generally, the financial instrument should be understood as the denial of access to specified individuals or groups from a formal or informal financial system, network, or source of funding.

At first glance, the financial and economic IOPs appear similar; however, they are fundamentally different in scope, enabling instruments, and associated activities. The economic IOP is used at the political level to influence the behavior of another state or organization.⁹ This is normally achieved through foreign aid, trade agreements, tariffs, embargos, or



Air battle manager with 16th Airborne Command and Control Squadron monitors radar system on E-8 Joint STARS aircraft flying off coast of Florida, July 14, 2018 (U.S. Air Force/Marianique Santos)

economic sanctions. These actions tend to be broader in scope and political in nature as they impact entire nations. As a result, the economic instrument relies on the diplomatic instrument to carry out these actions.

The financial IOP relies heavily on the Department of the Treasury, in close cooperation with banks, corporations, organizations, and international partners, in order to protect U.S. financial systems, combat adversary actors, administer sanctions, and freeze assets. Treasury wields a significant amount of power through the USA PATRIOT Act, requiring foreign banks to establish a contact for receiving subpoenas, scrutinize deposits from residents of nations that do not cooperate with U.S. officials, and impose sanctions on banks that do not provide information to law enforcement agencies.¹⁰ Through the PATRIOT Act and the Banks Secrecy Act, Treasury's Financial

Crimes Enforcement Network requires financial institutions, as of May 2018, to know their customer and perform customer due diligence to ensure customers are not involved in illegal activity and to cooperate with government agencies to detect and prevent money laundering.¹¹ Leveraging key mission partners enables the U.S. Government to prevent or deny access to financial systems to those actors that threaten national interests.

The financial IOP tends to be more agile in nature as it can specifically target countries, organizations, companies, and individuals utilizing banking systems to project power. A disruption of funding for a target entity can be achieved through compelling private banking institutions to deny currency loans or credit; blacklisting individuals, corporations, or states; utilizing financial sanctions; or freezing assets.¹² Disruptions are made possible because of U.S. worldwide

dominance in the financial sector. In 2014, the U.S. dollar was involved in 87 percent of the world's foreign exchange transactions, proof of its ability to influence financial institutions to comply.¹³ The intelligence IOP often pairs with the financial to detect and contain, and then the financial IOP deters and disrupts target adversary individuals or groups. The financial and intelligence IOPs are closely linked, delivering more precise effects related to financial systems and funding, whereas the economic IOP is tied to the diplomatic IOP, broader in scope and related to interstate commerce.

The benefit and relevance of the financial IOP is its precision. When targeting specific actors, the United States can achieve desired effects by focusing on critical vulnerabilities and capabilities without suffering second- and third-order effects caused by the economic IOP. This in turn can reduce the suffering of the



Afghan and coalition security force members conceal themselves in field during operation in search of Taliban facilitator in Sayyid Karam District, Paktia Province, Afghanistan, June 5, 2013 (U.S. Army/Codie Mendenhall)

population and improve U.S. legitimacy and credibility. The focus of the financial IOP has historically been VEOs, but it applies to all problem sets. In 2017, the United States targeted North Korea's ability to generate funds by potentially "suspending U.S. correspondent account access to any foreign bank that knowingly conducts or facilitates significant transactions tied to trade with North Korea or certain designated persons."¹⁴ In 2018, the restoration of sanctions on Iran targeted financial institutions, companies, and individuals tied to Iran's shipping, financial, and energy sectors, resulting in 700 additional companies and individuals on the sanction rolls, causing concern from the Iranian public and flaming potential unrest toward the regime.¹⁵

After the Ukraine conflict, the Office of Foreign Assistance Control created a blacklist to paralyze the financial dealings of a Russian billionaire friendly to the Kremlin, blocking transactions and payments from his bank by JPMorgan Chase, Visa, and MasterCard at a Russian embassy in Kazakhstan.¹⁶ In an attempt to halt Chinese global

investment, mergers to steal intellectual property, technology, and sensitive data, the Trump administration recently expanded the power of the Committee on Foreign Investment in the United States. National security reviews now include transactions in which a foreign investment was merely a minority interest instead of a controlling share and extend review powers into the real estate sector. Similarly, citing national security concerns, Australia, Canada, the European Union, France, Germany, Japan, and the United Kingdom have all joined an unprecedented global backlash against Chinese capital. Although many U.S. peer competitors tend to have nationalized industries, they must participate in the global market in order to be profitable, thus making them vulnerable to exploitation via the financial IOP. In turn, the use of these actions can result in slowing peer expansion and protecting U.S. national interests.

Intelligence. The multifaceted nature of intelligence makes it difficult to define. However, intelligence can be broadly broken down into three parts:

activities, products, and organizations. The organizations participate in the activities of "collection, processing, integration, analysis, and interpretation of available information" of hostile or potentially hostile forces that result in intelligence products.¹⁷ Activities are often associated with processes (such as the Joint Intelligence Preparation of the Operational Environment process, the targeting process, the intelligence process, etc.), as well as intelligence disciplines.¹⁸ The products are typically intelligence estimates and assessments that are often broken down into categories and could be in the form of written documents or verbal presentations, hard-copy publications, or electronic media.¹⁹ Organizations can be broken down into Department of Defense (DOD) agencies, other national agencies, foreign agencies, host-nation or local sources, and corporations. According to Craig Mastapeter in his Naval Postgraduate School thesis, "The intelligence instrument, or element, of national power integrates foreign, military, and domestic capabilities through policy, personnel, and technology

actions to provide decision advantage to policymakers, diplomats, financiers and economists, strategic communicators, warfighters, homeland security officials, and law enforcement.”²⁰ A more succinct and functional definition of the intelligence IOP that corresponds to both the joint concept and Mastapeter’s definition is the products, interdisciplinary activities, and organizations that convert disparate data about the environment, future capabilities and intentions, and relevant actors into coherent information to provide decision advantage for decisionmakers, both policymakers and commanders.

The term *intelligence* is often confused by operators and planners with the term *information*. Fortunately, the recent designation of information as a new joint function helped to shed some clarity on the difference in terms. As with all instruments of power, there is overlap, but the major difference is in the purpose, players, audience, and activities involved in each instrument. The focus of the intelligence IOP is the production of value-added data for the commander or decisionmaker to make informed decisions. Distinctly, the focus of the information IOP is to affect decision-making in the cognitive, informational, and physical dimensions of the target audience—whether friendly, neutral, or adversary—to create a desired effect.²¹ For example, the intelligence IOP may provide the critical information necessary for the commander to make a decision whereas the information IOP would help to create a desired effect in the target audience. Ultimately, the intelligence IOP provides decision advantage, and the information IOP is meant to influence a target audience.

The intelligence IOP involves many mission partners, all with varying and important missions articulated in the following categories: national agencies, allied partners and agencies, host-nation resources, and private sources. The U.S. Government has 17 national agencies with different mission sets utilized for intelligence-sharing and cooperation. Allied partners provide partnerships for intelligence-sharing and verification. Partner nations assist with local intelligence, while

the private sector provides independent investigation and analysis.

Access, speed, insight, the ability for direct action, and cover for U.S. interests are the advantages of utilizing mission partners outside of the United States.²² Commanders, however, must be judicious in their use of the foreign intelligence and host-nation and private-sector entities due to the disadvantages of conflicting interests, hostile collection, poor information gathering, and moral hazards.²³

It is vital to refocus U.S. intelligence efforts from the VEO threat to peer competition with Russia and China. Since 9/11, the reorganization of U.S. intelligence agencies has proved vital in disrupting terrorist and criminal organizations. To dismantle the VEO and criminal networks and neutralize high-value individuals, the U.S. Government and military have focused intelligence at the operational and tactical level for the past 20 years, relying heavily on intelligence, surveillance, and reconnaissance; dynamic targeting; and nodal analysis. The National Intelligence Council’s *Global Trends Report* indicates that the blurring of peacetime and wartime, the ease of disruption caused by nonstate groups, increase in standoff and remote attack capabilities, and new concerns about nuclear weapons and weapons of mass destruction are shaping conflicts that are more “diffuse,” “diverse,” and “disruptive.”²⁴ The 2019 National Intelligence Strategy provides some guidelines on the trends and focus areas such as strategic intelligence, anticipatory intelligence, current operations intelligence, and cyber threat intelligence.²⁵

The United States will need to harness the intelligence instrument to meet the new environment. Indications and warning intelligence as well as counter-intelligence will be critical to enable U.S. military and information instruments. Intelligence will need to emphasize attribution to identify criminal cyber and proxy actors that enable financial and law enforcement instruments to act. Data superiority and managing artificial intelligence and machine learning will

be necessary to navigate the sea of big data and to select and combine data in useful ways for decisionmaking. Finally, information-sharing between agencies and partnerships with external agencies and nations will be paramount to optimize intelligence activities, make faster decisions, and create unity of effort with mission partners.

Law Enforcement. Under the current DIME construct, the diplomatic and military IOPs’ legal efforts are not sufficient and are extremely complex. As a result, a separate IOP is necessary. The law enforcement IOP is challenging to define because it has two parts (legal and enforcement); encompasses the political, strategic, operational, and tactical levels; operates through other IOPs;²⁶ and relies heavily on national, international, foreign state, and local partners and organizations. Unlike other IOPs, the legal IOP is complex, incredibly diverse, and rapidly changing over short periods of time. A functional definition of the *law enforcement IOP* is the understanding and adherence to national, international, and local laws and the activities to support or carry out the enforcement of those laws and thereby restore order.

The *law* portion of law enforcement pertains to the legal expertise required to understand national law, international law, and foreign laws. This aspect is more strategic in nature and requires synchronization with the diplomatic instrument to avoid missteps in international and host-nation legal systems, carefully balancing the laws and interests of all national, international, and foreign entities. The *enforcement* aspect requires law enforcement agencies to work closely via the diplomatic IOP with data from the intelligence IOP to prosecute crimes and conduct activities at the tactical level through the military IOP or local law enforcement.

There are many key mission partners involved with the law enforcement IOP that include national, international, and foreign legal departments and law enforcement agencies.

The key U.S. organizations for the legal aspect are the Department of State and Department of Justice, which

provide legal expertise for national and international law while working with partner-nation justice departments to achieve an understanding of key legal issues. U.S. agencies, regional agencies, intergovernmental organizations, and host-nation partners are critical to enforcing laws and protecting the population. Through the diplomatic, intelligence, and financial IOPs, the law enforcement IOP is able to balance enforcing U.S. national laws and sovereignty with adhering to international law to maintain legitimacy while proactively detaining criminals to protect U.S. citizens and assist mission partners with their security needs.

A key U.S. strength is its alliances and leadership in the international system. U.S. competitors seek to attack partnerships, use the international system to slow actions, and delegitimize efforts across the globe. U.S. military legal expertise should broaden to international law and be incorporated into planning (not just law of armed conflict and rules of engagement). Commanders should also incorporate legal expertise from State or Justice into planning. Commanders could improve U.S. legitimacy with strategic communication, clarifying the message that the United States wants to enable countries to establish their own rules of law and improve their security and stability. Additionally, peer competitors increasingly use proxy, cyber, and criminal actors. International law and international law enforcement are key capabilities for defeating terrorist and adversary networks that span multiple national boundaries. It is therefore critical to reinforce whole-of-government, international, and interorganizational partnering to quickly identify, locate, and detain criminals anywhere on the globe, shortening our observe-orient-decide-act loop compared to our competitors and communicating attribution while defending U.S. national interests. The law enforcement IOP is crucial to achieving legitimacy by balancing national, international, and foreign law with national interests and partnering with local law enforcement entities to achieve unity of effort and accomplish objectives.

Recommendations: Putting the FIL into DIME

The DIME construct is overused and outmatched in our current environment. In order to perform in the competitive environment and navigate the gray zone, a full understanding of all IOPs is necessary. A more polished understanding of the new FIL IOPs is required to achieve unity of effort. In order to address the gap in understanding the FIL IOPs, it is critical to define concepts, incorporate them into doctrine, identify the appropriate mission partners, and apply DIME-FIL to the competitive environment. The following recommendations will improve the understanding and implementation of the DIME-FIL framework and allow the U.S. military to address the global problem sets, ultimately achieving unity of effort and effectively protecting national interests.

Update Joint Doctrine with DIME-FIL. The acronym *DIME-FIL* is colloquially being used in the joint lexicon, but the term has not been specifically defined or included in doctrine. Definitions provide the foundation for a common understanding of concepts and terms. The preliminary definitions addressed for the finance, intelligence, and law enforcement instruments provide a solid starting point to incorporate and update joint doctrine related to strategy, concepts, and planning. A clear definition can assist in the understanding, application, and synchronization of the IOPs for unity of effort in a competitive environment. Some logical publications to address the gap by defining, explaining, or listing the FIL IOPs are *Joint Doctrine Note 1-18, Strategy; Joint Publication (JP) 1, Doctrine for the Armed Forces of the United States; JP 3-08, Interorganizational Cooperation; and the Joint Concept for Integrated Campaigning.*

Identify the Mission Partners Involved with Each Instrument and Incorporate Them Early and Often in Planning. Planners and commanders are tasked with implementing the concept of global integration and executing different types of missions across the

spectrum that will be transnational, all domain, and multifunctional, so agility is key. Each line of effort will require a distinct and harmonious combination of the IOPs. Having a solid understanding of the key mission partners and their strengths across the DIME-FIL will enable commanders and planners to develop more creative plans that share the mission, tasks, and successes through a whole-of-government, international, and interorganizational approach. Incorporating partners early into planning will garner mutual trust and buy-in from partners who have a better understanding of their particular instruments. The U.S. military has more resources and planning experience compared to other agencies and partners, which provide a tremendous opportunity to coordinate, synchronize, and harmonize the instruments and subsequently the mission partners involved.

Train and Plan with DIME-FIL for Near-Peer Threats. Training should not be singularly focused on the big *M* and conventional warfare. Opening the aperture and adding more instruments of power to the U.S. lexicon signal that warfare has changed and that all instruments and partners are necessary for success. Planning should seriously consider harmonizing DIME-FIL, whole-of-government, and interorganizational concepts in the U.S. peer competition environment to compete in the gray zone and address U.S. problem sets. The DIME-FIL concept is a natural progression to a globally integrated approach that could be achieved through incorporating the key mission partners of all instruments in interorganizational exercises, the global campaign plan, and stability operations planning. These instruments should focus on creating effects on adversary critical capabilities and vulnerabilities, many of which will not be military in nature. Some key themes that may help us in the new environment are partnerships, strategic messaging, legitimacy, information sharing, decision advantage, technology, attribution, and tempo.

Additional IOPs have been identified, along with key mission partners,



Coalition-aligned security force Maghawir al-Thowra seize \$3.5 million in illicit drugs, including nearly 850,000 regional amphetamine Captagon pills, used to fund so-called Islamic State operations, in southern Syria, October 23, 2019 (U.S. Army/Kyle Alvarez)

that have the potential to result in better resource utilization, diversity of thought, and smoother transitions. It is the responsibility of planners and commanders to synchronize the instruments and create a more strategic globally integrated approach. The current doctrinal approach stymies the understanding of new IOPs, leaving commanders with plans that result in a limited conceptualization, a lack of creativity, and an echo chamber of DIME-centric operational approaches. By defining each of the FIL instruments, identifying key mission partners, and determining its application in the near-peer environment, commanders and planners are able to achieve understanding and apply the DIME-FIL framework to their way of thinking and approaching complex problem sets. The key aspect of the financial instrument is the denial of access to financial systems, mainly through

the Treasury Department, providing precision effects and denying adversaries access to financial systems. The intelligence instrument delivers decision advantage through activities, products, and organizations, mainly through national and international intelligence agencies, enabling value-added data for the rest of the IOPs. The two-pronged law enforcement instrument focuses on adherence to and enforcement of laws mainly through State and Justice, as well as DOD, granting the United States authority and legitimacy to take action and enabling the United States to detain criminals and restore order.

The “America First” strategy relies on U.S. partners to do more, which requires joint planners and commanders to leverage all resources, capabilities, and instruments in a concerted effort to achieve a more safe, stable, and secure world. The increased understanding

of the FIL IOPs allows the joint community to update doctrine, synchronize, and involve mission partners early in planning and perform in the competitive environment, ultimately achieving unity of effort and effectively protecting national interests. The DIME-FIL concept lends legitimacy to the U.S. cause and utilizes global integration to synchronize efforts, compete, and win in the strategic environment. JFQ

Notes

¹ Katerina Oskarrson and Robin Barnett, “The Effectiveness of DIMEFIL Instruments of Power in the Gray Zone,” *Open Publications* 1, no. 2 (2017), 8.

² Joint Doctrine Note 1-18, *Strategy* (Washington, DC: The Joint Staff, 2018), available at <https://fas.org/irp/doddir/dod/jdn1_18.pdf>; Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*

(Washington, DC: The Joint Staff, March, 2013), available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf>; JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 2013), available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf>; JP 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 2013), available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf>.

³ *National Strategy for Combating Terrorism* (Washington, DC: The White House, 2003), 15, available at <<https://fas.org/irp/threat/ctstrategy.pdf>>.

⁴ *Military Strategic Plan for the Global War on Terrorism* (Washington, DC: The Joint Staff, February 1, 2006), 6, available at <<https://archive.defense.gov/pubs/pdfs/2006-01-25-Strategic-Plan.pdf>>.

⁵ *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: The Joint Staff, September 10, 2012), 4, available at <www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cjco_jointforce2020.pdf?ver=2017-12-28-162037-167>.

⁶ Chairman of the Joint Chiefs of Staff Instruction 3100.01D, *Joint Strategic Planning System* (Washington, DC: The Joint Staff, July 20, 2018), A-1, available at <www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203100.01D.pdf?ver=2018-08-10-143143-823>; *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Edge* (Washington, DC: Department of Defense, 2018), 4, available at <<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>>.

⁷ Financial systems can include formal banking, informal systems, online value storage transfer systems, or cash couriers. See *National Strategy for Combating Terrorism*, 15.

⁸ Carl Priechenfied, “Untying Our Hands: Untying Cyber as an Instrument of National Power,” Master’s thesis, Joint Advanced Warfighting School, 2017, available at <www.hndl.org/?abstract&cid=805121>.

⁹ The relationship with the state or organization could be adversarial, neutral, or friendly.

¹⁰ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act*, Pub. L. No. 107-56, 107th Cong., October 26, 2001, available at <www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>.

¹¹ “Customer Due Diligence Requirements for Financial Institutions; Final Rule,” *Federal Register* 81, no. 91 (May 11, 2016), available at <www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf>; Financial Crimes Enforcement Network (FinCEN), “FINCEN’s Mandate from Congress,” n.d., available at <www.fincen.gov/resources/statutes-regulations>.

¹² Craig W. Mastapeter, “The Instruments

Joint Publications (JPs) Under Revision (to be signed within 6 months)

- JP 1-0, *Personnel Support*
- JP 2-0, *Joint Intelligence*
- JP 3-0, *Joint Operations*
- JP 3-05, *Special Operations*
- JP 3-26, *Combating Terrorism*
- JP X-XX, *Joint Electromagnetic Spectrum Operations*

JPs Revised (signed within last 6 months)

- JP 1, *Doctrine for the Armed Forces of the United States, Vols. 1 and 2*
- JP 3-31, *Joint Land Operations*
- JP 3-40, *Countering WMD*
- JP 5-0, *Joint Planning*
- JP 6-0, *Joint Communications System*

of National Power: Achieving the Strategic Advantage in a Changing World,” Master’s thesis, Naval Postgraduate School, 2008, 237–240.

¹³ Leah McGrath Goodman and Lynnley Browning, “The Art of Financial Warfare: How the West Is Pushing Putin’s Buttons,” *Newsweek*, April 24, 2014, available at <www.newsweek.com/2014/05/02/art-financial-warfare-how-west-pushing-putins-buttons-248424.html>.

¹⁴ Ankit Panda, “Trump Administration Introduces New Executive Order on North Korea Sanctions,” *The Diplomat*, September 22, 2017, available at <[wwwthediplomat.com/2017/09/trump-administration-introduces-new-executive-order-on-north-korea-sanctions/](http://thediplomat.com/2017/09/trump-administration-introduces-new-executive-order-on-north-korea-sanctions/)>.

¹⁵ “Restored U.S. Sanctions on Iran Cover Shipping, Financial, and Energy Sectors,” CBS News, November 4, 2018, available at <www.cbsnews.com/news/restored-u-s-sanctions-on-iran-cover-shipping-financial-and-energy-sectors-2018-11-03/>.

¹⁶ Goodman and Browning, “The Art of Financial Warfare.”

¹⁷ JP 2-0, GL-8.

¹⁸ This includes all of the intelligence disciplines—geospatial, human, signals, measurement and signature, and so forth.

¹⁹ Some example categories include warning intelligence, current intelligence, target intelligence, estimative intelligence, counterintelligence, and so forth.

²⁰ Mastapeter, “The Instruments of National Power,” 228.

²¹ JP 3-13, *Information Operations* (Washington, DC: The Joint Staff, November 27, 2012, Incorporating Change 1, November 20,

2014), available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf>. Summarized on page x and detailed in entire publication.

²² Erik Rosenbach and Aki J. Peritz, “Intelligence and International Cooperation,” Belfer Center for Science and International Affairs, July 2009, available at <www.belfercenter.org/publication/intelligence-and-international-cooperation>.

²³ Ibid.

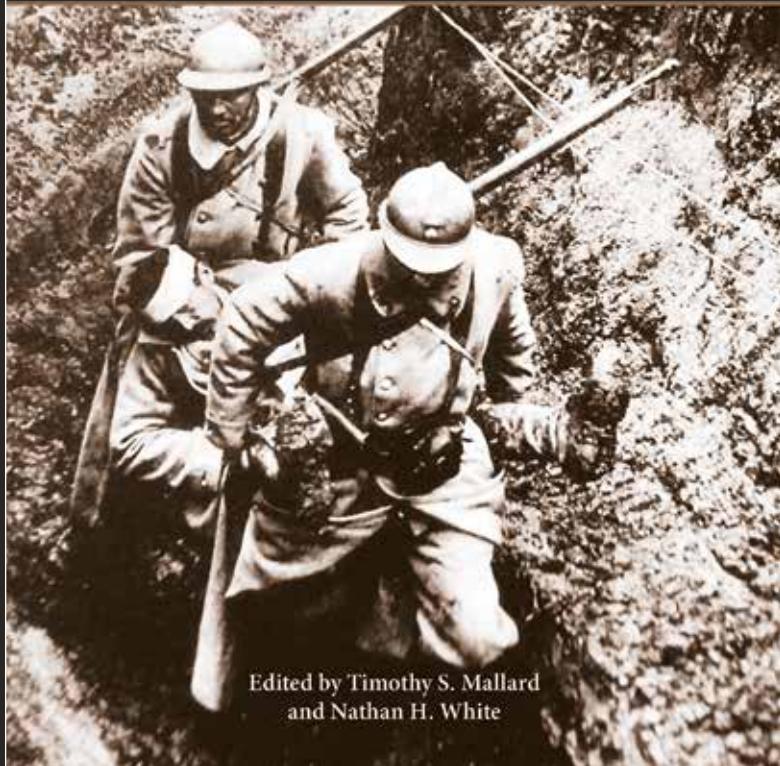
²⁴ *Global Trends: Paradox of Progress* (Washington, DC: National Intelligence Council, January 2017), 215–221, available at <www.dni.gov/files/documents/nic/GT-Full-Report.pdf>.

²⁵ *National Intelligence Strategy of the United States of America* (Washington, DC: Office of the Director of National Intelligence, 2019), available at <www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf>.

²⁶ The diplomatic, intelligence, and military instruments enable the law enforcement instruments of power.

A PERSISTENT FIRE

The Strategic Ethical Impact of World War I
on the Global Profession of Arms



Edited by Timothy S. Mallard
and Nathan H. White

New from NDU Press

A Persistent Fire: The Strategic Ethical Impact of World War I on the Global Profession of Arms

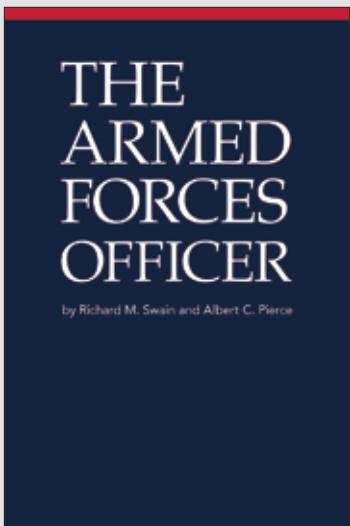
Edited by Timothy S. Mallard and Nathan H. White
2020 • 412 pp.

Since “the war to end all wars” witnessed the rise of global war among competing nation-states conducted in often tenuous alliances with nascent professional militaries—characteristics that continue to mark contemporary warfare a century later—then studying that conflict’s impact seems a relevant method to decide ways in which the profession of arms will develop in the next 25 to 50 years. Indeed, like a smoldering, persistent fire that threatens to re-erupt into a fresh conflagration, World War I continues to deeply shape and guide the profession of arms today.

Download the EPUB, MOBI, or PDF version for free.



Scan the QR Code above or go to:
<https://ndupress.ndu.edu/Publications/Books/A-Persistent-Fire>



From NDU Press
The Armed Forces Officer
2017 • 212 pp.

From the Foreword by General Joseph F. Dunford, Jr.:

"In 1950, the great Soldier-Statesman George C. Marshall, then serving as the Secretary of Defense, signed a cover page for a new book titled *The Armed Forces Officer*. That original version of this book was written by none other than S.L.A. Marshall, who later explained that Secretary Marshall had 'inspired the undertaking due to his personal conviction that American military officers, of whatever service, should share common ground ethically and morally.' Written at the dawn of the nuclear age and the emergence of the Cold War, it addressed an officer corps tasked with developing a strategy of nuclear deterrence, facing unprecedented deployments, and adapting to the creation of the Department of Defense and other new organizations necessary to manage the threats of a new global order.

"This new edition of *The Armed Forces Officer* articulates the ethical and moral underpinnings at the core of our profession. The special trust and confidence placed in us by the Nation we protect is built upon this foundation. I commend members of our officer corps to embrace the principles of this important book and practice them daily in the performance of your duties. More importantly, I expect you to imbue these values in the next generation of leaders."

Available at ndupress.ndu.edu/Media/News/Article/1159223/the-armed-forces-officer/

Have you checked out NDU Press online lately?



With 20,000 unique visitors each month, the NDU Press Web site is a great place to find information on new and upcoming articles, occasional papers, books, and other publications.

You can also find us on:



Facebook



Flickr



Twitter



Pinterest

Visit us online at: <https://ndupress.ndu.edu>



JFQ

JOINT FORCE QUARTERLY

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

