



JFQ | Joint Force Quarterly

Issue 110, 3rd Quarter 2023

Strategic Inflection Point

An AI-Ready Workforce

Analyzing a Country's Strategic Posture

Joint Force Quarterly

Founded in 1993 • Vol. 110, 3rd Quarter 2023
<https://ndupress.ndu.edu>

GEN Mark A. Milley, USA, Publisher

Lt Gen Michael T. Plehn, USAF, President, NDU

Editor in Chief

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

Executive Editor

Jeffrey D. Smotherman, Ph.D.

Senior Editor and Director of Art

John J. Church, D.M.A.

Internet Publications Editor

Joanna E. Seich

Copyeditors

Caroline Schweiter

Book Review Editor

Brett Swaney

Designer

Marco Marchegiani, John Mitrione,
U.S. Government Publishing Office

Advisory Committee

Lt. Gen. Dagvin R.M. Anderson, USAF/The Joint Staff; Col. Matthew O. Berry, USAF/Air Command and Staff College; Maj. Gen. Thomas D. Crimmins, USAF/Joint Forces Staff College; Brig. Gen. William C. Freeman, USAF/Air War College; RADM Peter A. Garvin, USN/U.S. Naval War College; MG David C. Hill, USA/U.S. Army War College; Ambassador (Ret.) Greta C. Holtz/College of International Security Affairs; Cassandra C. Lewis/College of Information and Cyberspace; LTG Theodore D. Martin, USA/U.S. Army Command and General Staff College; LTG James J. Mingus, USA/The Joint Staff; MajGen Paul J. Rock, USMC/National War College; MajGen William H. Seely III, USMC/Dwight D. Eisenhower School for National Security and Resource Strategy; Col Brian P. Sharp, USMC/Marine Corps War College; Col Bradford W. Tippet, USMC/Marine Corps Command and Staff College

Editorial Board

Richard K. Betts/Columbia University; COL Karen L.T. Briggman, USA/Dwight D. Eisenhower School for National Security and Resource Strategy; Eliot A. Cohen/The Johns Hopkins University; Jeremiah R. Dancy/U.S. Naval War College; Aaron L. Friedberg/Princeton University; Bryon Greenwald/National Defense University; COL James E. Hayes, USA/National War College; Col. Eric M. Murphy, USAF/Dwight D. Eisenhower School for National Security and Resource Strategy; Paul J. Springer/Air Command and Staff College; Bert B. Tussing/U.S. Army War College

Cover 2 images (top to bottom): Air Force Academy cadet Ben Charlebois competes in pole vault competition during Twilight Open at Cadet Outdoor Track and Field Complex in Colorado Springs, Colorado, May 5, 2023 (U.S. Air Force/Justin R. Pacheco); Air Force Academy cadet Rachel Crytser competes in 10-runner women's race during Twilight Open at Cadet Outdoor Track and Field Complex in Colorado Springs, Colorado, May 5, 2023 (U.S. Air Force/Justin R. Pacheco); Air Force's Marcell McCreary drives past University of Wyoming's Ethan Anderson at Clune Arena at U.S. Air Force Academy in Colorado Springs, Colorado, January 17, 2023 (U.S. Air Force/Trevor Cokley)



In This Issue

Dialogue

- 2 Letter to the Editor

Forum

- 4 Executive Summary
- 6 Strategic Inflection Point: The Most Historically Significant and Fundamental Change in the Character of War Is Happening Now—While the Future Is Clouded in Mist and Uncertainty
By General Mark A. Milley
- 16 A Framework for Lethal Autonomous Weapons Systems Deterrence
By Steven D. Sacks
- 26 Cutting the Chaff: Overlooked Lessons of Military UAP Sightings for Joint Force and Interagency Coordination
By Luke M. Herrington
- 35 Quantum Computing: A New Competitive Factor with China
By Doug Quinn, Patrick Wolverton, and Scott Storm

JPME Today

- 46 An AI-Ready Military Workforce
By Iain Cruickshank
- 54 Enhancing National Security: Increasing Female Faculty in Professional Military Education Would Strengthen U.S. Security
By Magdalena Bogacz

Commentary

- 61 Why Military Space Matters
By Gregory Gagnon
- 64 Improving Analytic Tradecraft: The Benefit of a Multilateral Foundational Training Model for Military Intelligence
By Eric Daniels
- 69 The Purpose and Impact of the U.S. Military HIV Research Program
By Joseph S. Cavanaugh, Clinton K. Murray, David Chang, and Julie A. Ake

Features

- 75 Special Operations Forces Institution-Building: From Strategic Approach to Security Force Assistance
By Kevin D. Stringer
- 88 Analyzing a Country's Strategic Posture: Suggestions for Practitioners
By Beatrice Heuser
- 98 Integrating Women, Peace, and Security Into Security Cooperation
By Barbara Salera
- 108 The Exceptional Family Member Program: Noble Cause, Flawed System
By Benjamin T. Bryant

Recall

- 118 The Civil War and Revolutions in Naval Affairs: Lessons for Today
By David C. Gompert and Hans Binnendijk

Book Reviews

- 130 China's Civilian Army
Reviewed by Ian Forsyth
- 131 Four Battlegrounds I, Warbot
Reviewed by Frank G. Hoffman
- 133 America's Great-Power Opportunity
Reviewed by Thomas F. Lynch III
- 135 Alpha
Reviewed by Paula G. Thornhill

Joint Doctrine

- 137 Mission Assurance: Decisionmaking at the Speed of Relevance
By Ari Fisher



About the Cover

Marine Corps Lance Corporal Jose Garcia-Gonzalez, intelligence specialist with Maritime Surveillance Platoon, 3rd Intelligence Battalion, III Marine Expeditionary Force Information Group, holds security during field exercise at Jungle Warfare Training Center, Camp Gonsalves, Okinawa, Japan, on September 12, 2022 (U.S. Marine Corps/Manuel A. Serrano)

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

3rd Quarter, July 2023
ISSN 1070-0692



Assistant Secretary of Defense John Plumb and Army General Paul Nakasone, commander of U.S. Cyber Command, prepare their testimony for House Armed Services Committee, in Washington, DC, March 30, 2023 (DOD/E.J. Hersom)

Letter to the Editor

The April 2023 issue of *Joint Force Quarterly* includes a positive review of our recent book, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, by Stafford Ward, as well as an article on cyber and deterrence by James Van de Velde. Readers, both those who follow the cyber and deterrence discussion closely and those new to the topic, might be confused by the two pieces and their disparate representation of U.S. Cyber Command's operational approach of persistent engagement and how it fits with a strategy of deterrence and with the more recent concept of integrated deterrence. As theorists writing on cyber persistence and a practitioner implementing persistent engagement, we offer some clarification.

Stafford Ward's review accurately describes our thesis, derived from historical experience, that states misunderstanding the technical, tactical, and operational features of the strategic environment in which they seek security may suffer strategic losses in competition, crisis, and armed conflict. We introduced the analytical construct of three strategic environments—conventional, nuclear, and cyber—in which each relies on a distinct logic for producing security. In cyberspace, security rests primarily on the strategic principle of initiative persistence in exploitation—anticipating the exploitation of one's own vulnerabilities, leveraging the capacity to exploit others' vulnerabilities, and seizing and sustaining

the initiative in this exploitation dynamic. Security in this interconnected space of constant contact and fluid technological terrain requires continuous maneuvering against adversaries to gain insights about adversary tactics, techniques, and procedures. These insights can be shared with government and industry partners at home and abroad to enable them to proactively inoculate vulnerable assets from cyber exploitation, disruption, and destruction, leading to increased and improved resiliency and defense. These insights can also be used to preclude, inhibit, and otherwise constrain adversaries from cumulating strategic gains.

Deterrence, which rests on prospective threat to react (through threat of either punishment or attritional denial), has failed as a strategy in cyberspace both to support resiliency and defense and to dissuade states from pursuing strategic gains cumulatively in and through cyberspace below the level of armed conflict. Cyber operations and campaigns conducted in competition are more than a nuisance or mere espionage—they can be strategically consequential. As an example, the North Koreans are undermining the effectiveness of the U.S.'s Ground-based Midcourse Defense System by funding North Korea's missile and nuclear programs via strategic cyber campaigns that manipulated digital financial transactions. This is why the Department of Defense and U.S. Cyber Command adopted the Defend Forward strategy and the operational approach of persistent engagement in

2018. The 2022 U.S. National Defense Strategy reinforces this paradigm shift in its call for campaigning below armed conflict to limit, frustrate, and disrupt competitor activities that seriously affect U.S. interests. In other words, persistent engagement is *not* the “operational implementation of cyber deterrence” as Van de Velde concludes. Persistent engagement is an alternative to a deterrence strategy. Although we argue in *Cyber Persistence Theory* that deterrence as a strategic approach may succeed against armed attack equivalent effects delivered in and through cyberspace, it patently does not provide security below that threshold, and an alternative approach based on a distinct strategic logic must guide the pursuit of security in that strategic space. When employed persistently over time, a “deterrent effect” might result from cyber campaigns, but this is not because one has applied a deterrence strategy.

These nuances are critically important for civilian and military scholars, policymakers, and students to grasp. Calling cyberspace operations “the operational implementation of cyber deterrence” is not only incorrect but also potentially distracting at a time when strategic clarity is required.

Cyber capabilities and operations must be leveraged to support integrated deterrence in a way that aligns with the reality of the cyberspace strategic environment. Unlike conventional and nuclear capabilities, cyber activities alone do not deter because they are not useful as a coercive

mechanism. This conclusion follows from empirical evidence and scholarly consensus. Accordingly, the best use of cyberspace capabilities and operations for integrated deterrence comes from their persistent use in “campaigning” against continuously active adversaries, working across boundaries (interagency, private sector, and allies) with all instruments of national power to set conditions to deter and prevail in crisis and conflict. Strategic value comes not from signaling intent and shaping decisionmaking in those moments but from advancing security through cyber means applied in competition to structure the crisis or fight.

There are several threads to setting conditions for crisis or conflict through campaigning. The first involves defensive activities to set the theater and globe for joint force operations. This includes mission assurance of one’s own networks, weapons, and systems, as well as coalition warfighting networks. The second thread is setting partnerships. As General Paul Nakasone articulated in his recent Vanderbilt University keynote address, “The winners of future competitions and conflicts will be those coalitions that can set conditions for dynamic collaboration with speed across a broader section of societies, regions, and sectors, fostering mutual understanding and congruent action.” The third thread is the effort to undermine the adversary’s desired crisis and warfighting conditions and constrain its freedom of maneuver. Campaigning in and through cyberspace can undermine an adversary’s confidence in its capabilities, complicate military preparations, counter information campaigns that aim to undermine U.S. public support and alliance cohesion, expose information and intelligence to deny the adversary control of the global narrative, and preclude or constrain opportunities through hunt-forward operations.

Examples of these threads include the hunt-forward operations in Montenegro to improve American cyber defenses ahead of the 2020 election and those in Ukraine to provide and receive insights to/from Ukrainian operators while also inoculating U.S. systems from Russian cyber actors and any proxies supporting its war against Ukraine. Additionally, after

discovering a massive Russian botnet (CyclopsBlink) that had not yet been activated against U.S. national interests, the Federal Bureau of Investigation effectively dismantled the botnet in March 2022. Finally, U.S. cyber-enabled campaigns through public release of intelligence have been credited with ensuring alliance stability for a coordinated effort to compel Russia to cease its aggression.

In our book, as Ward notes, we are cautious in making claims that cannot be supported by evidence or compelling logic. Cyber is a novel capability that has never been used in a militarized crisis between nuclear-armed peers. In a crisis, uncertainty invites miscalculation and inadvertent escalation, and novel cyber actions could introduce a bevy of uncertainties in signaling, effects, shared understandings of the severity of effects, and commitment. The assertion that cyber provides “off-ramps” to deescalate crisis is untested, unproved, not empirically supported, and counter to theories of crisis bargaining. We do not know whether cyber options in a crisis would signal lack of resolve or if they would deescalate or escalate the situation. While cyber has proved to be nonescalatory in day-to-day competition between nuclear-armed peers, this does not ipso facto mean cyber is nonescalatory or deescalatory in a crisis.

Finally, we urge readers to recognize that these arguments are more than purely academic—they inform decisions about resourcing, force structure, and mission. To that end, we disagree with Van de Velde’s claim that persistence in competition vies with posturing for contingency. The reality is far more nuanced. First, as we describe earlier, campaigning in competition enables warfighting. Second, there is a great deal of overlap and synergy between the requirements for day-to-day competition and posturing for contingency. For example, campaigning helps secure the Department of Defense information networks, readies the force, increases whole-of-nation resilience, uncovers targets of opportunity, and generates response options for use in crisis or conflict. There are indeed priorities specific to managing crisis and prevailing in conflict,

such as access to specialized hard targets and the bespoke tools to exploit those targets. Although effort must surely be expended on tailored accesses and capabilities, campaigning helps ensure they can be brought to bear in the event of crisis and armed conflict. Campaigns in competition are not less consequential than actions in crisis and armed conflict, as implied by the figures in Van de Velde’s article.

Cyberspace requires us to rethink the competition-conflict continuum, which is often depicted linearly from competition to crisis to conflict, with risk increasing as one moves along the continuum. The implication is that war presents the greatest risk of strategic loss, and therefore everything we resource and execute in competition is weighed against the likelihood of escalation to war, as well as how it postures and prepares us for war. As argued in *Cyber Persistence Theory*, competition in and through cyberspace can hold the same strategic import as armed conflict. Thinking about competition principally as a step toward armed conflict neglects the ways in which actions in competition can secure strategic victory without ever having to engage in armed conflict.

We appreciate Stafford Ward’s encouraging *JFQ* readers to examine our book for a fuller discussion of cyber competition, deterrence, initiative persistence, and persistent engagement. We agree with the National Defense Strategy and James Van de Velde that ensuring adversaries cannot use conventional force, nuclear threats, and exploitative cyber campaigns to undermine U.S. power certainly requires an integrated approach. But contrary to Van de Velde’s suggestion, one must also acknowledge that different approaches are needed for different threats. Initiative persistence is not deterrence—it is distinct and, if pursued well, complementary and supportive. *JFQ*

Michael P. Fischerkeller, Researcher, Institute for Defense Analyses; Emily O. Goldman, Cyber Strategist at U.S. Cyber Command; Richard J. Harknett, Chair, Center for Cyber Strategy and Policy at the University of Cincinnati



Marine assigned to 3rd Reconnaissance Battalion, 3rd Marine Division, conducts high altitude, low opening parachute jump from Air Force C-130J Super Hercules assigned to 36th Airlift Squadron, over Yokota Air Base, Japan, December 13, 2021, as part of weeklong joint training using Air Force and Navy aircraft (U.S. Air Force/Yasuo Osakabe)

Executive Summary

Since Vietnam and importantly over a decade later—with the establishment of the requirements for joint operations, the joint force concept, and the idea of jointness with the Goldwater-Nichols Department of Defense Reorganization Act of 1986—we have witnessed a slow but important shift in how the United

States and its coalition partners address conflicts locally and globally.

Having grown up in the post-Vietnam-era U.S. Air Force, riding in the most high tech aircraft of the day, interoperating with multiple Services and multiple nations as a daily part of our tactical operation that had a strategic impact, I had a front row seat to what could be done

if Service- or Nation-dominant positions were set aside to see how each participant could leverage everyone else's strengths to positive mission accomplishment.

Despite the obvious size and influence of the Services on the development of weapon systems and the organizing of their warfighting capabilities, their separate cultures have not fully prevented

those who can see the requirement to better integrate these Service formations, from the command level all the way down to the tactical, from advocating for true jointness. The largest and most successful parts of jointness to date can be seen in the combatant commands and their daily control over joint operations, in the success of joint professional military education in helping foster an understanding of the value of working together as a joint and combined team, and in the growing efforts at the Department of Defense to bring industry, government, and warfighters from all the Services, as well as our Allies and partner nations, together to innovate both technological solutions and human development for the benefit of all.

Jointness isn't just an option. It is essential and required for mission success. Jointness enables successes like Operations *Desert Storm* and *Allied Force*. Even in crisis, joint and combined efforts ultimately result in the best outcomes when victory isn't possible in a classic sense. We all might value the capabilities of the Service we signed up for, but each is only a part of a bigger and much more powerful force when we all work together. I would offer that jointness is what our military needs more of to assure our success in the future. Each of us should see our role as an advocate for jointness because to do otherwise lessens the value and contribution of our own Service teammates and those from the other Services, our allies, and our partners. Most importantly, you will see that the Chairman, after 43 years in the U.S. Army, sees jointness as the only way to go.

Our Forum section welcomes four separate cutting-edge articles on 21st-century warfighting led by the Chairman of the Joint Chiefs of Staff, General Mark Milley, as he provides the joint force his views on the evolving Joint Warfighting Concept and its place in the soon-to-be-released accompanying joint doctrine. His call for the establishment for a Joint Futures Command and for increased jointness by design is certainly a welcome development to this veteran of the former

Joint Forces Command. With the rise of increasingly autonomous weapons systems, Steven Sacks provides his take on how they fit into a conceptual framework of deterrence. After a series of encounters with unidentified aerial phenomena (UAPs, as UFOs are now known), Luke Herrington helps us sort through how to improve interagency coordination in dealing with these events. Following on to several articles *JFQ* has recently published, Doug Quinn, Patrick Wolverton, and Scott Storm suggest quantum computing as one of our advantages in our competition with China.

We offer the ideas of two professors in this edition's JPME Today. With the distinct buzz globally about the rise of artificial intelligence, the Army Cyber Institute at West Point's Iain Cruickshank helps us learn the best way to recruit the right people into the military who can best take advantage of this brave new world ahead. Seeing a distinct advantage in diversifying the gender of JPME faculties, Magdalena Bogacz describes the positive and lasting impact this change will have on national security. In my own tenure teaching at NDU, I can see the slow but positive climb in female faculty and the definite positive impacts this is having. How could it not?

This edition's Commentary articles take us to all parts of the military experience, from space to intelligence to the battle against HIV/AIDS. If you are wondering where the U.S. Space Force needs to go in order to wage the Nation's battles on the ultimate high ground, the Service's "Two" who leads their intelligence staff, Gregory Gagnon, discusses the need for better integration of all allied and joint force capabilities, leveraging and relying on military space forces primarily more than in past conflicts in part due to the challenges that China poses in all domains, but especially in space. Career intelligence professional Eric Daniels provides us with his thoughts on how to improve intelligence training across the joint force. Although many of us have long ago forgotten about the HIV/AIDS crisis, the team of Joseph Cavanaugh, Clinton Murray, David

Chang and Julie Ake describe how the Department of Defense is still actively involved in preventing and combating HIV/AIDS.

In Features, the focus is on the human dimension of the joint force and strategy, with both new and familiar authors. First of two returning *JFQ* alumni, Kevin Stringer brings his wealth of experience to help us understand how to move from an operational approach to employment of special forces in security force assistance operations. Once again, we welcome internationally known strategy expert Beatrice Heuser, who offers her views on how we can assess a country's position in the global strategic environment. Seeing women as the frequently overlooked "secret weapon," Barbara Salera provides a positive approach to security cooperation, which many of our allies have already adopted. Closer to home, Benjamin Bryant offers a studied critique of the Defense Department's Exceptional Family Member Program.

Rounding out this issue of *JFQ*, our Recall article takes us back to the Civil War as David Gompert and Hans Binnendijk tie how the rapid development and experimentation in naval operations and armaments then have significant and useful concepts for today's force. In Joint Doctrine, Ari Fisher believes there is a better way to help commanders assess how ready their force is to fight. To these excellent articles we add four book reviews, and we hope you will find useful new ideas to add to your professional understanding and development.

Your voice in how best to move the joint force forward can only help achieve both the mission of this journal and the goals of the new Joint Warfighting Concept. Every successful leader at every level knows the wisdom of how to bring diverse talents together to achieve the mission. The Chairman and *JFQ* are looking for your ideas on how to achieve success together as we deal with the world today and in the future. *JFQ*

—William T. Eliason,
Editor in Chief



Strategic Inflection Point

The Most Historically Significant and Fundamental Change in the Character of War Is Happening Now—While the Future Is Clouded in Mist and Uncertainty

By General Mark A. Milley

Geostrategic competition and rapidly advancing technology are driving fundamental changes to the character of war. Our opportunity to ensure that we maintain an enduring competitive advantage is fleeting. We must modernize the Joint Force to deter our adversaries, defend the United States, ensure future military advantage, and, if necessary, prevail in conflict. The Joint Force has taken the first step by developing and publishing the Joint Warfighting Concept (JWC) and updating Joint Publication 1, Doctrine for the Armed Forces of the United States. The JWC is a joint, combined vision for how the U.S. military will operate across all domains. The next step is to create a leadership structure that turns concepts into capabilities. The Joint Force must make fundamental changes now to win the next war and, by doing so, we will deter the war from happening in the first place.

General Mark A. Milley is the 20th Chairman of the Joint Chiefs of Staff.



U.S. Coast Guard—manned LCVP from USS *Samuel Chase* disembarks troops of Company A, 16th Infantry, 1st Infantry Division, wading onto Fox Green section of Omaha Beach, early on June 6, 1944 (U.S. Coast Guard/Robert F. Sargent); *Der Wanderer über dem Nebelmeer*, by Caspar David Friedrich, oil on canvas, ca. 1817 (Hamburger Kunsthalle); Drone swarm (Shutterstock/Chesky); Army Futures Command IVAS Concept Art, circa 2019 (U.S. Army)

paratroopers and glider infantry drifted down to the coast of France. The continuous roar from the 88mm guns pierced the serenity of the night. The stream of lead from the German MG-42s raked the beaches of Normandy. For many American Soldiers, the taste of saltwater and the sharp smell of gunpowder were their first experiences of combat. These brave troops answered our nation's call to defend freedom and democracy. The cost was tremendous. Twenty-six thousand Americans were killed in action from the storming of Normandy to the liberation of Paris. Between 1914 and 1945, 150 million people were slaughtered in the Great Power wars of World War I and World War II.

Since 1945, there have been several limited and regional wars, but there has not been another Great Power war. There are many reasons for this outcome. Two of the most important reasons are the rules-based international order enforced by a network of allies and partners and the dominant capability of the U.S. military. This order has held for almost eight consecutive decades. Unfortunately, we now see tears in the fabric of the rules-based international order as adversarial global powers continuously challenge the system. The time to act is now.

The U.S. military's purpose is simple and contained in our oath to support and defend the Constitution against all enemies, both foreign and domestic, and to protect the American people and our interests. Since World War II, the strength of our nation and military, alongside that of our allies and partners, has deterred Great Power war. Freedom is not guaranteed. As Ronald Reagan warned, "Freedom is a fragile thing and it's never more than one generation away from extinction. It is not ours by way of inheritance; it must be fought for and defended constantly by each generation."²

In 2023, the rules-based international order is under intense stress.

Simultaneously, we are witnessing an unprecedented fundamental change in the character of war, and our window of opportunity to ensure that we maintain an enduring competitive advantage is closing. What we do in the next few years will set conditions for future victory or defeat. The U.S. military is the most effective fighting force the world has ever known, but maintaining this advantage is not a given. There are two critical areas where the Joint Force must adapt now:

- a conceptual roadmap—a unifying *joint* operational vision—that deliberately drives future force development and design
- a leadership structure to turn that vision into reality.

Changing Character of War

The rapid change in the character of war demands a corresponding fundamental shift in our Joint Force. As Carl von Clausewitz stated, the *nature* of war—a violent contest of wills to achieve political aims—is immutable. Humans will continue to impose their political will on opponents with violence. Clausewitz also tells us the nature of war involves fear, friction, uncertainty, and chance inherent in the dynamic interaction among the government, the people, and the military.

However, the *character* of war—how, where, with what weapons, and technologies wars are fought—is changing rapidly.³ For example, the last fundamental change in the character of war occurred between World War I and World War II. Technological advancements fundamentally transformed the character of warfare: mechanization and the use of wheeled and tracked vehicles; widespread employment of the aircraft, including development of bombers and fighters; and proliferation of radio to coordinate and synchronize dispersed units. The way militaries conducted warfare—the *character*—shifted drastically

When we look to the future, we can see broad outlines, but the details are clouded in fog and mist. Our path is rarely clear and never certain. Nevertheless, we must make choices for the future of the Joint Force. We know we will not get it right, but we must strive to get it less wrong than the enemy, paraphrasing the late historian Michael Howard.¹ The new Joint Warfighting Concept (JWC) is our guide to that future. It will drive our doctrine, organizational design, training, and ultimately warfighting itself.

This is not the first time we have adapted to address an uncertain future. Seventy-nine years ago, on June 6, 1944, ordinary Americans came from all walks of life to enter the crucible of combat. Over 154,000 troops from eight Allied nations boarded 6,000 vessels to cross the choppy English Channel. As the moon illuminated the night sky, 24,000 Allied

and drove a change in organizational structure, training, and leadership development. The nations that capitalized on these changes created the greatest advantages in battle.

Almost all developed nations had access to these technologies—Great Britain, France, Germany, the Soviet Union, Japan, and the United States—but it was only the German Wehrmacht that initially optimized all three technological advancements, combining them into a way of war called Blitzkrieg that allowed them to overrun Europe in just 18 months.⁴ Germany eventually lost to the overwhelming industrial might of the United States, in conjunction with the Soviet Union and other Allies, but we may not get 18 months to react to a future enemy onslaught.

Today, we are witnessing another seismic change in the character of war, largely driven again by technology. The next conflict will be characterized by ubiquitous sensors with mass data collection and processing ability that minimize the opportunity for military forces to hide. Low-cost autonomous platforms, coupled with commercial imagery and behavior tracking data augmented by artificial intelligence (AI) and analysis tools, will accelerate the ability to sense and make sense of the environment. Inexpensive drones, loitering munitions, and precision-guided munitions with increasing speed, range, and accuracy will further reduce the time it takes to close the kill web. Robotics and additive manufacturing will change the way militaries supply and sustain their forces. Pervasive sensors, AI-driven weapon systems, and long-range precision fires will make the fastest platforms seem slow and leave the most hidden formations exposed.

Finally, the increasing development of space and cyber platforms and capabilities, both kinetic and nonkinetic, ensure the next war's decisive terrain will not be limited to the earth's surface. In short, the battlefield fundamentals of see, shoot, move, communicate, protect, and sustain are changing in fundamental ways. The attributes of organizations will—by necessity—be small, widely dispersed, nearly autonomous and self-sustaining,

capable of constant motion, and able to periodically mass effects for decisive action. This operational environment will place a premium on decentralized mission command. Centralized micromanaged leadership from the top will be ineffective. The American homeland has almost always been a sanctuary during conflict, but this will not be the case in a future war. Robust space and cyber capabilities allow adversaries to target critical national infrastructure. We cannot be sure that adversaries will ethically constrain emerging technologies or restrain their use of weapons of mass destruction.⁵

The Joint Force is actively harnessing these technologies, but as the Russian invasion of Ukraine has shown, technology alone does not guarantee success in the next war. The Joint Force must adopt innovative technology; modernize or divest older systems; train, organize, and equip the warfighter in new ways; update our doctrine to be effective in the operating environment; develop resilient leaders who can successfully conduct operations with little guidance and execute the true meaning of mission command; and work as a truly joint and combined team. But we are not adapting fast enough to optimize the force and keep pace with the changing character of war. We must adapt much faster than we are doing now.

Changing Global Order

The global geopolitical situation has also changed fundamentally. During the Cold War, there were two competing superpowers. After the fall of the Berlin Wall, there was a brief so-called unipolar moment. Now, it is clear we are in a multipolar world with at least three Great Powers—the United States, China, and Russia—with other countries rapidly emerging as regional and potential global Great Powers. We can say with reasonable certainty the future will be increasingly complex. Additionally, the rules-based international order established 80 years ago is currently under tremendous strain. The United States now faces two nuclear armed powers. Therefore, we must do everything in our power to deter conflict. We

may be in competition and confrontation, but we are not yet in conflict.

The 2022 National Security Strategy (NSS) identifies the People's Republic of China (PRC) as "America's most consequential geopolitical challenge" and its "pacing challenge."⁶ More specifically, the National Defense Strategy (NDS) states that the PRC is a revisionist power that employs state-controlled forces, cyber and space operations, and economic coercion against the United States and its allies and partners.⁷ In 2018, it was reported that China's President Xi Jinping stated to the 13th National People's Congress in Beijing, "We are resolved to fight the bloody battle against our enemies . . . with a strong determination to take our place in the world."⁸ China seeks to fundamentally revise the system while still operating within it.

The world is also facing the greatest shift in economic power in well over 100 years. The PRC has leveraged economic growth to invest heavily in its military with the stated intention of exceeding the capability of the U.S. military in the Western Pacific in the next decade and globally by 2049.⁹ Through economic coercion, the PRC is expanding its global footprint and increasing its ability to project military power at range and scale. In addition, it is aggressively modernizing its military to develop nuclear, space, cyber, land, sea, and air capabilities to erode the competitive advantages that the United States and its allies have enjoyed for decades. The PRC's goal is to revise the global international order by mid-century and become the regional Asian hegemon in the next 10 years. The PRC is taking increasingly aggressive action toward those ends with a publicly unambiguous national aspiration and roadmap. This represents a real and growing national security challenge for the United States and its allies. While the PRC is an increasingly capable strategic competitor, history is not deterministic, and war is neither inevitable nor imminent. It is important that we keep our relationship with the PRC at the level of competition and not allow it to escalate into conflict.



British "Experimental Company" participates in Project Convergence 22, Fort Irwin, California, November 4, 2022 (Courtesy British Army/ Donald C. Todd)

While the PRC is the Joint Force's pacing challenge, Russia poses an acute threat. The NSS warns that Russia "poses an immediate and ongoing threat to the regional security order in Europe."¹⁰ Russia is a revanchist actor seeking to return to an era when it dominated the "Near Abroad" in a 19th- and 20th-century imperial system.¹¹ Furthermore, Russia employs disinformation, cyber, and space operations against the United States and irregular proxy forces in multiple countries.¹²

Russia's unprovoked and illegal invasion of Ukraine in February 2022 has caused untold human suffering. Vladimir Putin's war of choice not only threatens peace and stability on the European continent but is also a frontal assault on the basic rules of the post-World War II United Nations Charter. Ukraine has been an independent country since 1991. Russia's war of aggression to redraw country borders is an existential threat to Ukraine and a direct threat to the North Atlantic Treaty Organization (NATO) and the rules-based international order. The United States and many of its allies and partners are supporting Ukraine with

materiel and training to ensure that the international order is upheld.

Both China and Russia threaten Asian and European geopolitical stability and the international order.¹³ The challenge is likely to increase in the years ahead.

A Unifying Joint Vision: The Joint Warfighting Concept

The changing character of war and geopolitical landscape requires an interoperable, multidomain capable, joint and coalition force to demonstrate credible integrated deterrence. To remain the most lethal military in the world, the Joint Force needs a unifying concept and a faster process to field required capabilities. This means we also need authorities and a leadership model that drive deliberate Joint Force Development and Joint Force Design.

The most important thing we can do is to deter Great Power war from happening in the first place. We achieve deterrence by maintaining a highly ready, combat capable force in the present and modernizing the U.S. military to sustain dominant warfighting advantage in a

future operating environment. When rational adversaries view the United States as dominant, they realize they cannot and should not engage in conflict with the United States. Implementing a joint warfighting concept is the best preparatory action to deter adversarial actors from military aggression and preserve peace.

The JWC is our roadmap to the future. It is a threat-informed, operational concept that provides an overarching approach to how the Joint Force should fight in a future conflict. After 4 years of focused development, wargaming, and experimentation, the latest version of the JWC provides a unifying vision for the Department of Defense (DOD) to *guide* Joint Force Development and Joint Force Design, *drive* DOD investment, and *inform* how we work in concert with allies and partners. The JWC is nested directly under the NSS, NDS, and National Military Strategy (NMS), so it also describes *how* the Joint Force will address the top four DOD priorities: defend the homeland, deter strategic attacks against the United States and its allies and partners, deter



aggression while being prepared to prevail in conflict, and ensure our future military advantage. Most importantly, it challenges the warfighter to make a fundamental shift in the way we think about maneuvering through space and time in a fast-paced, high-tech, rapidly changing, and exceptionally challenging and lethal environment.

The JWC's lineage traces back to the AirLand Battle (ALB) concept and doctrine developed in the 1970s and 1980s. In the 1970s, the U.S. Army and NATO Allies faced the threat of

a conventional war in Europe against a numerically superior Soviet Union and its alliances through the Warsaw Pact. After witnessing the modern high-intensity conflict of the October 1973 Arab-Israeli Yom Kippur War, Army planners recognized that NATO and U.S. forces in Europe required new ideas of force employment.¹⁴ The subsequent ALB concept reintroduced the operational level of war in its theory of winning decisive first battles on the ground and then conducting precision air interdiction of Soviet echelons.¹⁵

The Army introduced ALB in the 1982 edition of Army Field Manual 100-5, *Operations*, and it dominated Army design, development, and education for the next decade.

ALB served as an example of successful bottom-up efforts; however, while ALB achieved collaborative force design and development between the Army and Air Force, it did not create necessary jointness to overcome conflicting visions of airpower and responsibility for long-range fires, nor did it incorporate significant roles for maritime forces.¹⁶



Air Force Technical Sergeant patrols with Ghost Robotics Vision 60 prototype at simulated austere base during Advanced Battle Management System exercise on Nellis Air Force Base, Nevada, September 3, 2020 (U.S. Air Force/Cory D. Payne)

The JWC describes how the Joint Force will operate across not only the air and land domains but also multiple domains (land, sea, air, space, and cyber) and systems. The JWC also provides Joint Force Design with enough flexibility to drive experimentation, exercise, and training of the Joint Force, while leveraging Service iteration and innovation. This JWC is truly *joint*.

Evolution of Concepts

In 1996, *Joint Vision 2010* claimed technology trends would change the

character of war: “By 2010, we should change how we conduct the most intense operations. Instead of relying on massed forces and sequential operations, we will achieve massed effects in other ways.”¹⁷ Key terms included *dominant maneuver*, *precision engagement*, *full-dimensional protection*, and *focused logistics*.¹⁸ The main idea that emerged—effects-based operations—changed the way we think about warfare.

By 2005, the *Capstone Concept for Joint Operations (CCJO) 2.0* recognized “dominance” may not be assured, so it

called for the Joint Force to think differently and act from multiple directions in multiple domains concurrently, conduct integrated and independent actions, project and sustain the force, act directly on perceived key elements and processes in the target system, control tempo, transition quickly and smoothly among the various actions, manage perceptions and expectations, and act discriminately.¹⁹ To accomplish this, the concept demanded certain traits of the future warfighter, including networked, interoperable, resilient, agile, and lethal.²⁰

In 2012, the *Capstone Concept for Joint Operations: Joint Force 2020* recognized “the conventions by which wars are fought are no longer as settled as they once were. Notions of who is a combatant and what constitutes a battlefield in the digital age are rapidly shifting beyond previous norms.”²¹ In response, the concept proposed a new approach: globally integrated operations²² with eight elements: mission command; seize, retain and exploit the initiative; global agility; partnering; flexibility in establishing joint forces; cross-domain synergy; use of flexible, low-signature capabilities; and increasingly discriminate to minimize unintended consequences.²³ Similarly, the 2012 *Joint Operational Access Concept* called for cross-domain synergy with a “more flexible integration of space and cyberspace operations into the traditional air-sea-land battlespace than ever before.”²⁴ We knew over 10 years ago that a fully functioning Joint Force would need to outmaneuver, outthink, and outpace malign actors by remaining agile and working as a truly joint team.

Over the past 25 years, we have learned significant lessons. Whereas the 1996 *Joint Vision 2010* called for “full spectrum dominance,” we know now that we cannot assume dominance in any domain. Where the 2005 *CCJO* assumed the Joint Force could move in multiple directions in multiple domains, we now know the Joint Force should not expect freedom of movement. In 2012, the *CCJO: Joint Force 2020* called for mission command but lacked mention of joint all-domain command and control.

The JWC builds on these lessons learned. We now have a truly joint all-domain concept. Next month, we will release Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*. This updated doctrine will guide the Joint Force in how to fight in the years ahead.

Key Tenets of JWC and JP 1

- *Integrated, Combined Joint Force:* The concept emphasizes the need for seamless integration of all mili-

tary Services across all warfighting domains, enabling them to function as a unified force. This type of integration involves synchronized planning, shared situational awareness, and effective communication across different Service components, fully aligned and interoperable with key allies and partners.

- *Expanded Maneuver:* The expanding operating environment means the Joint Force must also practice expanded maneuver. The JWC challenges the warfighter to think creatively about moving through space and time, including—but not limited to—maneuver through land, sea, air, space, cyber, the electromagnetic spectrum, information space, and the cognitive realm.²⁵
- *Pulsed Operations:* A type of joint all-domain operation characterized by the deliberate application of Joint Force strength to generate or exploit our advantages over an adversary.
- *Integrated Command, Agile Control:* Seamless command and control across all domains. Effective command and control aims to integrate sensors, platforms, and decisionmaking processes to achieve real-time battlespace awareness and enable rapid decisionmaking.
- *Global Fires:* Integration of lethal and nonlethal fires to deliver precise, synchronized global effects across all domains and multiple areas of responsibility.
- *Information Advantage:* Leveraging advanced technologies, such as AI, big data analytics, and cyber capabilities, to collect, analyze, and disseminate information rapidly, enabling decision superiority and action.
- *Resilient Logistics:* A system that allows for rapid movement of personnel, equipment, and supplies to places and times of our choosing.

In addition to the tenets, the JWC also highlights individual and organizational *attributes*. We need our warriors, through selection and training, to possess the traits of agility, rapid decisionmaking, creativity, dispersed

teamwork, and extreme resiliency in the face of intense hardship and continuous isolation. Future warfighting attributes must include speed, constant motion, relatively small size, lethality, and self-sustaining autonomous or nearly autonomous abilities. Warfighters must be masters of technological and physical camouflage, concealment, and deception.

Capability Development

While the Joint Force has naturally evolved over the years to identify and procure capabilities through processes and forums like the Joint Requirements Oversight Council (JROC), the Joint Force still lacks an organizational structure—or a coach with the right authorities—to hold the team accountable. The JWC, in and of itself, will not produce the objective Joint Force we need in the future. As aspects of the JWC are validated through rigorous experimentation and analysis, those pieces of the concept must be translated into military requirements, both materiel and nonmateriel. Moreover, they must be fully integrated across DOTMLPF-P before we achieve a true operational capability.²⁶ The JROC is where this happens. It validates these requirements and ensures we have the right people, equipment, training, leader development, and doctrine to deter and, if necessary, win in a future conflict.

Since its establishment in 1986, the JROC has primarily operated through a bottom-up process where combatant commands identified critical gaps in their operational employment concepts and the military Services sponsored requirements to fill those warfighter gaps. Over the last 4 years, the Vice Chairman of the Joint Chiefs of Staff, in collaboration with the Service vice chiefs, has focused the JROC on balancing nearer term combatant command needs with the pressing requirement to modernize the Joint Force. The JWC has been the North Star to this process, providing a list of Concept Required Capabilities—critical elements that enable concept execution. Moreover, in 2022, the JROC drove alignment of capability portfolio management with Office of



X-47B Unmanned Combat Air System demonstrator flies near aircraft carrier USS *George H.W. Bush*, May 14, 2013 (U.S. Navy/Erik Hildebrandt)

the Secretary of Defense integrated acquisition portfolios to further streamline procurement processes across DOD.

A Future-Focused Organization for Force Development and Design

The JWC and JP 1 have established a path to modernization. But these alone will not achieve the fundamental changes required to ensure the Joint Force outpaces any adversary and continues to deter aggression. In addition to these reforms, we need a future-focused organization that can drive change. In the 2022 NMS, we highlighted the need to balance both modernizing the Joint Force for future warfare and campaigning today in an era of Great Power competition.²⁷ The Joint Force can strike this balance by using strategic discipline—the ruthless prioritization of operations, activi-

ties, and investments to continuously calibrate Joint Force weight of effort between campaigning now and rapidly building warfighting advantage for the future.²⁸ It could seem like a struggle to balance “fight tonight” against “prepare to win tomorrow,” but it is a false choice between current readiness and future modernization—we must do both with the assistance of a Joint Futures organization.

Army Futures Command (AFC) is proof that a future-focused organization can spark the changes required. The AFC model can be replicated at the joint level. It achieved undeniable momentum in delivering advanced capabilities to the warfighter faster. The Army established a four-star operational commander as an authoritative senior advocate for the future—combining the characterization of the future operating environment, concept development, experimentation,

and requirements generation with clear priorities and direction. Unlike decades of failed programs like Comanche, Crusader, and Future Combat Systems, the Army is now putting the newest and most innovative technology in the hands of Soldiers. Like AFC, a Joint Futures organization would have the potential to align critical force design and development functions, integrate concepts with experimentation, and synchronize users to accelerate modernization and close capability gaps.

A Joint Futures organization would drive future Joint Force Design. It would be responsible for *characterizing* the future joint operating environment, looking beyond the current Future Years Defense Program. Building on the success of the JWC and JP 1, this organization would develop and iterate on future joint warfighting concepts. It would ensure capability development is threat informed



B-21 Raider is unveiled at public ceremony, December 2, 2022, in Palmdale, California (U.S. Air Force); Saildrone Explorer unmanned surface vessel and guided-missile destroyer USS *Delbert D. Black* operate in Arabian Gulf, January 8, 2023 (U.S. Navy/Jeremy Boan)

and concept driven. This organization would not monopolize joint concept development but rather serve as a lead agency that is responsible for collaborating with the Services and combatant commands to identify and help prioritize future operational problems while synchronizing development of warfighting solutions.

This future-focused organization would prioritize *joint experimentation* to ensure joint concepts are validated through rigorous wargaming, modeling, simulations, and other experimentation. This would strengthen Joint Force Design through competition of ideas, leveraging Service, industry, and academic innovation efforts. It would create experimentation venues to evaluate innovative tactical and operational solutions to inherently joint problems.

This organization would *integrate with allies and partners* from the very beginning of force design, looking to enhance not only the Joint Force but also the coalition force, through

synchronization and integration of coalition design and development. Allies and partners give the United States an asymmetric advantage over competitors. Thus, including them in force design and development allows us to integrate and inform capability development across nations in a way that reduces redundancies, leverages strategic competitive advantages, and strengthens the coalition force, enhancing our alliances and security partnerships and, ultimately, strengthening integrated deterrence.

Finally, and most importantly, we would designate the leader of this organization as the senior advocate solely dedicated to focus on the future joint operating environment, concepts, force design, requirements, and doctrine. He or she would represent the future joint warfighter in decision forums. This leader and organization would maintain a persistent focus on the fundamental evolution required for our future Joint Force.

Conclusion

Nearly 2,500 years ago, Thucydides warned, “It would be a mistake for you to think that because of your city’s present military might, or because of the gains you have made, luck will always go your way. Prudent men preserve their gains with a view to the uncertainty of the future and this makes them able to deal with disaster more intelligently when it comes.”²⁹ We do not want disaster; we want to deter war, but if it comes, this Joint Force must be prepared to prevail.

The Joint Force faces an uncertain future, and the challenges are multifaceted, complex, rapidly approaching, and unrelenting—demanding comprehensive modernization of our forces, concepts of employment, supporting technology, infrastructure, and training. We are undertaking several initiatives to transform, such as the JWC, JP 1, and JROC revitalization, and developing a joint organization focused solely on the



future, unencumbered by current crises and near-term constraints.

I leave my post as the Chairman of the Joint Chiefs of Staff this fall, and after nearly 44 years of military service, I am confident that we will remain the most lethal, resilient, and capable force the world has ever seen, but we need to fundamentally change the way we do business, and we need to do it now. JFQ

Notes

¹ Michael Howard and A.J. Wilson, "Military Science in the Age of Peace," *RUSI Journal* 119, no. 1 (March 1974), 4.

² Ronald Reagan, "January 5, 1967: Inaugural Address (Public Ceremony)," Ronald Reagan Presidential Library and Museum, <https://www.reaganlibrary.gov/archives/speech/january-5-1967-inaugural-address-public-ceremony>.

³ Hew Strachan and Sibylle Scheipers, eds., *The Changing Character of War* (Oxford: Oxford University Press, 2011); Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), book 1, chapter 1, 88–89.

⁴ Andrei A. Kokoshin, *The German Blitz-*

krieg Against the USSR, 1941 (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, June 2016), <https://www.belfercenter.org/sites/default/files/files/publication/Blitzkrieg%20Final.pdf>.

⁵ *Defense Panel Interim Panel Report: The Future of Conflict and the New Requirements of Defense* (Arlington, VA: Special Competitive Studies Project, October 2022), <https://www.scspp.ai/wp-content/uploads/2022/10/Defense-Panel-IPR-Final.pdf>.

⁶ *National Security Strategy* (Washington, DC: The White House, 2022), 11, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.

⁷ *2022 National Defense Strategy of the United States of America* (Washington, DC: The Joint Staff, 2022), <https://www.defense.gov/National-Defense-Strategy/>.

⁸ James Griffiths, "China Ready to Fight 'Bloody Battle' Against Enemies, Xi Says in Speech," CNN, March 20, 2018, <https://edition.cnn.com/2018/03/19/asia/china-xi-jinping-speech-npc-intl/index.html>.

⁹ Edmund J. Burke et al., *People's Liberation Army Operational Concepts*, RR-A394-1 (Santa Monica, CA: RAND, 2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR394-1/RAND_RRA394-1.pdf. See also Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," speech delivered at 19th National Congress of the Communist Party of China on October 18, 2017, Xinhua, November 3, 2017, http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National-Congress.pdf.

¹⁰ Ibid.

¹¹ Gerard Toal, *Near Abroad: Putin, the West, and the Contest Over Ukraine and the Caucasus* (New York: Oxford University Press, 2017).

¹² *Defense Panel Interim Panel Report*.

¹³ *National Military Strategy 2022: Strategic Discipline* (Washington, DC: The Joint Staff, 2022), https://www.jcs.mil/Portals/36/NMS%202022%20_%20Signed.pdf.

¹⁴ Boyd L. Dastrup, *Modernizing the King of Battle: 1973–1991* (Fort Sill, OK: U.S. Army Field Artillery Center and School, 2003), https://history.army.mil/html/books/069/69-5-1/cmhPub_69-5-1.pdf.

¹⁵ Leon H. Rios, *The Linkage of the Strategic and Operational Levels of War* (Fort Leavenworth, KS: School of Advanced Military Studies, 1986), <https://apps.dtic.mil/sti/pdfs/ADA174246.pdf>.

¹⁶ Paul Benfield and Greg Grant, *Improving Joint Operational Concept Development Within the U.S. Department of Defense* (Washington, DC: Center for a New American Security,

October 2021), <https://www.cnas.org/publications/reports/improving-joint-operational-concept>.

¹⁷ *Joint Vision 2010* (Washington, DC: The Joint Staff, 1996), 17, <https://apps.dtic.mil/sti/pdfs/ADA311168.pdf>.

¹⁸ Ibid.

¹⁹ *Capstone Concept for Joint Operations Version 2.0* (Washington, DC: Department of Defense, August 2005), 16–20, <https://apps.dtic.mil/sti/pdfs/ADA476464.pdf>.

²⁰ Ibid., 20.

²¹ *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: The Joint Staff, September 10, 2012), 3, https://www.ndu.edu/Portals/59/Documents/Incoming/ccjo_2012.pdf.

²² Ibid., 4.

²³ Ibid.

²⁴ *Joint Operational Access Concept (JOAC) Version 1.0* (Washington, DC: Department of Defense, January 17, 2012), 16, https://dod.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf.

²⁵ Todd Schmidt, "The Missing Domain of War: Achieving Cognitive Overmatch on Tomorrow's Battlefield," *Modern War Institute*, April 7, 2020, <https://mwi.usma.edu/missing-domain-war-achieving-cognitive-overmatch-tomorrows-battlefield/>.

²⁶ While the official definition of DOTM-LPF-P comes from the *Joint Capabilities Integration and Development System Manual*, the Defense Acquisition University defines *DOTM-LPF-P* as Doctrine: the way we fight (for example, emphasizing maneuver warfare, combined air-ground campaigns); Organization: how we organize to fight (divisions, air wings, Marine Air-Ground Task Forces); Training: how we prepare to fight tactically (basic training to advanced individual training, unit training, joint exercises); Materiel: all the "stuff" necessary to equip our forces that *does not* require a new development effort (weapons, spares, test sets that are off the shelf both commercially and within the government); Leadership and education: how we prepare our leaders to lead the fight (squad leader to four-star officer, professional development); Personnel: availability of qualified people for peacetime, wartime, and various contingency operations; Facilities: real property, installations, and industrial facilities (government-owned ammunition production facilities); Policy: DOD, interagency, or international policy that impacts the other seven nonmateriel elements," <https://www.dau.edu/acquipedia/pages/ArticleContent.aspx?itemid=457>.

²⁷ *National Military Strategy 2022*.

²⁸ Ibid.

²⁹ Thucydides, *The Peloponnesian War*, trans. Walter Blanco, ed. Walter Blanco and Jennifer Tolbert Roberts (New York: W.W. Norton & Company, 1998), book 4, 151.



Marine Corps Lance Corporal Donte Mathews, rifleman with 1st Battalion, 8th Marine Regiment, 2nd Marine Division, flies unmanned aircraft system on Camp Lejeune, North Carolina, January 17, 2023 (U.S. Marine Corps/Michael Virtue)

A Framework for Lethal Autonomous Weapons Systems Deterrence

By Steven D. Sacks

As the United States and the People's Republic of China (PRC) continue down a path of increasing rivalry, both nations are investing heavily in emerging and dis-

ruptive technologies in search of competitive military advantage. Artificial intelligence (AI) is a major component of this race. By leveraging the speed of computers, the interconnectedness of the Internet of Things, and big-data algorithms, the United States and the PRC are racing to make the next leading discovery in the field. Both nations endeavor to incorporate AI

into weapons systems and platforms to form *lethal autonomous weapons systems* (LAWS), which are defined as weapons platforms with the ability to select, target, and engage an adversary autonomously, with minimal human inputs into their processes.¹ Without a clear framework through which to assess interactions between LAWS of different nations, the likelihood of accidental

Captain Steven D. Sacks, USMCR, is a Private-Sector Security and Risk Advisor based out of Washington, DC.

or inadvertent escalation to military crisis increases. *Accidental escalation* is an unintended consequence of events that were not originally intentional, whereas *inadvertent escalation* is a situation in which an actor's intended actions are unintentionally escalatory toward another.² This article explores how LAWS affect deterrence among Great Powers, developing a framework to better understand various theories' applicability in a competition or crisis scenario between nations employing these novel lethal platforms.³

Deterrence

In *Deterrence in American Foreign Policy*, Alexander L. George and Richard Smoke define *deterrence* as "simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh the benefits."⁴ The act of persuasion relies on psychological characteristics of the actors in a potential conflict scenario. By leveraging an understanding of an opponent's motivations to generate signals of allegedly guaranteed reactions the sending nation will take if provoked, that sending nation is signaling both its capability and its will to fight.⁵ Deterrence can be further broken down into *direct deterrence*, a state's dissuading an adversary from attacking its sovereign territory, and *extended deterrence*, the act of dissuading an aggressor from attacking a third party, usually a partner or ally.⁶ This article focuses on the latter, specifically looking at concepts that would be applicable to the U.S. attempt to deter the PRC from conducting aggressive military operations against a partner or ally in the Indo-Pacific region. The proffered framework also applies to scenarios in which the PRC attempts to deter the United States from third-party intervention subsequent to a fait accompli aggressive action against an American partner or ally.

According to George and Smoke's definition, to increase the effectiveness of deterrence a state must either increase the cost of the aggressor state's escalation or expand the overall risk of increased aggression within the relationship. James

Fearon's "tying hands" and "sinking costs" are two methods by which a country can signal to another its level of resolve if attacked. Tying hands links the credibility of political leadership to a response to foreign aggression; sinking costs involves deploying forces overseas, incurring *ex ante* costs that signal military resolve.⁷ Glenn Snyder further expounds on the sunk cost theory, introducing the idea of a "plate-glass window" of deployed troops that an aggressor must shatter to attempt any offensive action against a third country.⁸ The shattering of the plate-glass window is understood as an assured trigger for third-party intervention, exemplified historically by the U.S. decision in 1961 to deploy an Army brigade to West Berlin meant to deter a Soviet invasion of the city.⁹

The Department of Defense has defined the *endstate of deterrence* as the ability to "decisively influence the adversary's decisionmaking calculus in order to prevent hostile action against U.S. vital interests."¹⁰ To achieve this end, the U.S. military conducts global operations and activities that affect the ways adversaries view threats and risks to their own national security. More recently, American military leadership has emphasized deterrence as the desired endstate of a defending country's military strategy, separate and distinct from compellence.¹¹ Chinese scholars, in contrast, discuss deterrence as more analogous to Thomas Schelling's overall characterization of coercion, melding the concept of deterrence with that of compellence.¹² These scholars view deterrence in a similar manner to Maria Sperandei's "'Blurring the Boundaries': The Third Approach," acknowledging the often overlapping relationship between deterrence and compellence, in which one can easily be framed in the context of the other.¹³ Additionally, Chinese authors see deterrence as a milestone that supports setting conditions, which then enable the achievement of more strategic political endstates, rather than an endstate itself.¹⁴

Chinese military scholars have written about the use of limited kinetic force as a deterrent, showing the adversary an example of PRC military capabilities to

dissuade the potential aggressor from taking any actions.¹⁵ The use of kinetic weapons platforms as a deterrent likely increases the risk of *inadvertent escalation*, defined as when "one party deliberately takes actions that it does not believe are escalatory but [that] another party to the conflict interprets as such," thereby making the competition more volatile.¹⁶ Leaders within the People's Liberation Army (PLA) almost certainly view their introduction of AI and LAWS as contributing to competitive military advantage while simultaneously setting favorable conditions for conflict should the relationship escalate by deploying and employing these capabilities among PLA units.¹⁷ One concern with Chinese writings on deterrence is the yet-unreconciled tension between the dual goals of deterring escalation and simultaneously preparing the battlefield; they lack assessments regarding which deterrent activities risk interpretation as escalatory by their adversaries.¹⁸

Even as PLA writers look to the military application of AI to generate control, the lack of available scholarly work on how the United States will interpret its introduction is cause for concern.¹⁹ The PLA's theory of military victory is based on its ability to effectively control the escalation of the conflict, employing both deterrence and compellence principles to achieve strategic political goals in a predictable manner that leaves Beijing in the driver's seat of conflict.²⁰ Although a 2021 RAND report on deciphering Chinese deterrence signals establishes a framework by which the United States can better understand PLA military deterrence signals, a more comprehensive understanding of effective deterrent signaling between the United States and China remains elusive.²¹ As long as this gap persists, there remains a high risk of inadvertent escalation to major conflict due to misunderstanding as new technologies and capabilities are phased in to the militaries of both nations.

Employment of Autonomy in Warfare

AI is the employment of computers to enable or wholly execute tasks and/or decisions to generate faster, better,

or less resource-intensive results than if a human were completing the task. AI applies across disciplines, from conducting light-speed stock market trades to performing supply chain risk analysis. AI brings speed-of-machine decisionmaking that often frees human resources to focus on more complex tasks, making it a useful means within the current Great Power competitive dynamic to gain advantages against adversaries in a resource-constrained environment.²² The Chinese government has allocated increasing resources to the development of disruptive capabilities such as AI as a key pillar of its national strategy, leveraging science and technology as part of the PRC's pursuit of Great Power status.²³

AI encompasses a spectrum of capabilities that leverages computers to increase speed, reduce costs, and limit the requirement for human involvement in task and decision processes. Within AI, there are two concepts that play critical roles in understanding how LAWS affect conventional deterrence theory: machine learning (ML) and autonomy. ML employs techniques that often rely on large amounts of data to train computer systems to identify trends and analyze best courses of action.²⁴ An AI system's ability to learn depends on the quality and quantity of data. More pertinent data available across a wide spectrum of relevant scenarios allow the ML algorithms to train to handle a wider range of situations. The better the ML code training, the more autonomous a system can become. Regarding the second concept, autonomy, there exists a spectrum, from "human-AI co-evolving teams," in which both parties mature together on the basis of mutual interactions over long periods of time, to "human-biased AI executing effects," in which the autonomous platform reacts rapidly to its environment in a manner informed by human input and set parameters.²⁵ From enhancing logistics operations through predictive supply chain modifications to reducing commanders' uncertainty through sensor proliferation and programmed analysis, autonomous systems can provide significant benefits to militaries able and willing to incorporate them into emerging concepts of operations.²⁶

The use of LAWS in combat affects the application of deterrence through the manipulation of cost-benefit analyses conducted by the actors in conflict. Replacing human assets with unmanned equivalents diminishes the risk of human losses from military engagements, potentially changing the escalation calculus for militaries that place a high value on human life.²⁷ By decreasing the risk of human casualties, the introduction of LAWS may reduce the political barriers hindering a decision to launch escalatory military operations, thereby increasing the potential for large-scale conflict.²⁸ Reducing these barriers to escalation further increases the risk of inadvertent or accidental escalation, in combination with the uncertainties brought about by relegating increasing amounts of decisionmaking authority from humans to weaponized battlefield platforms. The effects of emerging and disruptive technologies and operations in the United States and the Soviet Union during the Cold War were counterbalanced and the situation stabilized through a mutually understood framework of deterrence. The advent of emerging and disruptive LAWS, combined with a lack of established messaging and signaling norms, is destabilizing to the future of the U.S.-PRC relationship.

One aspect of the introduction of autonomy to the battlefield that does not deal directly with deterrence but remains relevant is the potential for increased autonomy to result in degraded control of systems by human military commanders and leaders. Both Washington and Beijing have made it clear that human involvement in weapons systems engagement decisions remains a priority. In 2012, the Pentagon released a directive mandating that autonomous and semi-autonomous weapons systems be designed to allow humans appropriate oversight and management of the use of force employed by those systems.²⁹ These decisionmaking processes will also remain squarely within the legal boundaries of the codified rules of engagement and law of war. China's military has remained more ambiguous as to its stance on the use of autonomy in lethal warfare.

Beijing has both called for the prohibition of autonomous weapons, through a United Nations binding protocol in 2016, and issued its New Generation of AI Development Plan, in 2017—which served as the foundation for its development of autonomous weapons.³⁰ Both nations have shown hesitance to deploy fully autonomous lethal weapons systems to the battlefield; however, with emerging technologies and innovations, that reluctance may change.

Brinkmanship and Signaling

In *Arms and Influence*, Schelling describes brinkmanship as a subset of deterrence theory defined by two actors pushing the escalation envelope closer to total war; brinkmanship must include elements of "uncertainty or anticipated irrationality or it won't work."³¹ In the Cold War era, uncertainty was driven by human psychology and external actors—would a military leader take it upon him- or herself to make aggressive moves that might initiate a limited conflict, or would a third party take action that would force one of the belligerents to respond offensively? In the era of AI, ML, and LAWS, uncertainty is also derived from the unpredictability of the system code itself.³² The amount of trust practitioners can place in their LAWS is limited to the breadth, depth, and quality of the data and scenarios in which the platform is tested and evaluated—a concern because real-world combat often lies outside of training estimates.³³ The problem of amassing sufficient quantities of data with necessary fidelity and relevancy to future operations is compounded by the pace of the change to the character of warfare brought about by the implementation of AI and ML on the battlefield.³⁴ All of these factors challenge the ability to generate human trust in LAWS, given the increased levels of uncertainty about their predictable performance across a spectrum of military operations.³⁵

This uncertainty in the reliability of autonomous weapons presents a security dilemma among Great Powers because the side with more lethal platforms gains a greater first-strike advantage over time.³⁶



MQ-8B Fire Scout unmanned aircraft system from Helicopter Maritime Strike Squadron (HSM) 35 performs ground turns aboard littoral combat ship USS *Fort Worth*, South China Sea, May 1, 2015 (U.S. Navy/Conor Minto)

The speed at which computers make decisions also enhances the effect of autonomous unpredictability on brinkmanship.³⁷ Additionally, adversaries can hack LAWS code to degrade or deny operational capability, introducing further uncertainty into autonomous warfare.³⁸ An early example of autonomous unpredictability occurred in 2017, when the Chinese Communist Party developed automated Internet chatbots to amplify party messaging; the bots gradually began to stray off message, culminating in posts criticizing the party as “corrupt and incompetent” before officials took the software offline.³⁹

The concept of private information also contributes to uncertainty and brinkmanship. Private information is privileged knowledge about capabilities

and intentions known only to the originating country. Nations have an incentive to keep private information hidden from adversaries to generate a tailored external perception favorable to the owner of the information.⁴⁰ But countries can deliberately reveal private information to external actors through signaling—the sending of a calculated message to a target audience to convey specific information for a desired effect. To be successful, a signal must be received and interpreted as intended by the sender. State leaders and administrations, however, are prone to misperception because of inherent biases that influence their reception of signals.⁴¹ The ability to successfully signal capabilities and intentions regarding LAWS is complicated

by the uncertainty introduced by the employment of autonomous algorithms. There remains a dearth of research exploring how emerging robotics will potentially affect the successful conveyance of deterrent signals.⁴²

Separate but not necessarily distinct from the ability to signal capability while retaining the advantage of private information is the ability to signal intent. Experts including Robert Jervis have explored the ability of states to increase national security without falling victim to the security dilemma by developing overt distinctions between weapons systems with offensive versus defensive intents. Jervis writes, “When defensive weapons differ from offensive ones, it is possible for a state to make itself more secure



Digital recreation of Holloman High-Speed Test Track with ejection seat test setup created as part of Project Zero, in effort to train drones through machine learning to conduct automated, artificial-intelligent driven operations and data analysis, Holloman Air Force Base, New Mexico, June 6, 2022 (U.S. Air Force)

without making others less secure.”⁴³ Table 1 depicts the two variables Jervis assessed, offense-defense distinguishability and offense-defense advantage in conflict, to create quadrants describing “worlds” of risk conditions. This framework is especially applicable to overlay with current concepts of deterrence by punishment, where offense has the advantage, and deterrence by denial, where defense has the advantage.

Decisions by Washington and Beijing to prioritize private information and operations security surrounding the development and testing of LAWS inhibit the diffusion of technology to the private or commercial sector or to other national militaries, even when those external entities may have technological advantages over national military capabilities. By compartmenting the technology at the foundation of AI-enabled warfighting platforms, these decisions make it difficult to distinguish the military intent of these capabilities—whether they are for offensive or defensive posturing. Additionally, proprietary and

classified LAWS enhance first-mover advantage as each Great Power is racing to develop measures and countermeasures to provide its military a battlefield advantage.⁴⁴ This effect is further highlighted in Chinese military strategy, which stresses the importance of seizing and maintaining the initiative in conflict, often through rapid escalation across domains, before an adversary has a chance to react or respond—a *fait accompli* campaign.⁴⁵ An inability to distinguish defensive systems from offensive ones employed in a world where offensive first movers have the advantage places the situation in Jervis’s “doubly dangerous” world.

The inability to trace autonomous decision processes further challenges the ability to predict and understand the effectiveness of signaling through LAWS. Neural networks at the core of AI decisionmaking are characterized as “black boxes,” offering minimal insight into the impetus behind their autonomous assessments or decisions.⁴⁶ Without the ability to analyze how these

algorithms make decisions, engineers struggle to make reliable cause-to-effect assessments to determine how the autonomous systems can be expected to act in specific situations. Recent wargames have demonstrated that autonomous systems are less capable of understanding signals and therefore are more prone to unpredictable decision-making than humans. These systems are often programmed to maximize decision speed and to seek out perceived exploitable opportunities to capitalize on rapidly. These priorities make them more likely to escalate battlefield engagements in situations where a human would be reluctant to deviate from the status quo.⁴⁷ Deploying LAWS into the competition domain thus introduces novel signaling opportunities: the ability to overtly switch a weapons system to autonomous operation, unswayed by outside factors or emotions, can indicate military determination, taking the decision to initiate aggressive defensive

Table 1. Jervis’s Four Possible Worlds

	Offense Has the Advantage	Defense Has the Advantage
Offensive Posture Not Distinguishable from Defensive One	1 Doubly dangerous	2 Security dilemma, but security requirements may be compatible
Offensive Posture Distinguishable from Defensive One	3 No security dilemma, but aggression possible. Status-quo states can follow different policy than aggressors. Warning given.	4 Doubly stable

Source: Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics* 30, no. 2 (January 1978), 211.

actions out of human hands, should a preprogrammed red line be crossed.⁴⁸

There is the potential that the unpredictability in the LAWS decisionmaking process constitutes its own deterrent. In a scenario where the adversary cannot assess with confidence how an autonomous weapons system will act in a specific battlefield situation, there is the potential that the adversary will be dissuaded from initiating an attack for fear of an unknown ability that eclipses the adversary's own. However, a more effective use of unpredictability resides at the operational rather than the tactical level of warfare. By reliably revealing a new lethal autonomous capability during a large-scale demonstration or exercise, the United States can show that it has more operational options for military forces at its disposal.⁴⁹ There is a likelihood that the PRC will observe a new demonstrated capability and infer that the United States is concealing even more capable and lethal proficiencies.⁵⁰ Both of these effects would lend themselves to the conclusion that revealing a novel LAWS capability may have more deterrent impact than concealing it.

A Framework for Deterrence With Autonomous Weapons Systems

Two critical factors determine how LAWS affect deterrence in future warfare: predictable lethality of the weapons systems and effective signaling of that lethality to adversaries. Table 2

describes four possible permutations of deterrence through the use of LAWS in a naval blockade scenario. In these scenarios, a defending nation has established a naval blockade using LAWS deployed in permanent autonomous modes of operations by their human users and coded to engage any foreign platform that approaches within a set distance from the blockade. The aggressor state is advancing toward the blockade with manned platforms, threatening offensive action against the defender. The defending nation has attempted to signal to the aggressor that the unmanned blockade has been switched to autonomous mode and will attack the advancing adversary if it crosses the red line of proximity.

In the table's Tripwire Deterrence quadrant, the defending nation possesses predictability in the lethal autonomous weapons systems' ability to execute their decisionmaking processes as intended, and it has effectively signaled this capability to the advancing force. In this scenario, uncertainty is minimized; both sides understand the red line and how the autonomous blockade will react to a crossing. Because the role of humans is minimized in the decision loop of AI systems operating on the "human-biased" side of the autonomous spectrum, individual psychology and emotions do not inject unpredictability into the engagement, resulting in what Schelling describes as a defensive tripwire.⁵¹ In Tripwire Bluff, the defenders have

effectively signaled to adversaries the lethal autonomous weapons systems' predictable lethality; however, the purported predictability is not manifest in reality. Either the autonomous systems in the blockade are untested, or they have been tested with inconsistent results. In this scenario, the defender is successfully bluffing a tripwire defense to the adversary.

In Single-Side Uncertainty, the defender has confirmed predictable lethality from its blockade but has failed to effectively signal this capability to the advancing aggressor. In this scenario, the aggressor is unsure whether to believe that the blockade will operate as intended and is subsequently faced with making a decision handicapped by the uncertainty about the defender's true capabilities. In Brinkmanship Deterrence, the defending blockade does not possess predictable lethality, nor has the defender effectively communicated that capability to the adversary; both sides are uncertain how the blockade will react to aggressor action.

Of the scenarios described above, Tripwire Deterrence brought about by LAWS is the most stable because private information is minimized. In this context, both the sender and receiver of the deterrence signals understand the capabilities of the autonomous weapons platforms and know under what conditions these platforms will initiate action against an adversary. Tripwire Bluff situations are stable only so long as the nation receiving the deterrence signal does not become privy to the unpredictability of the autonomous

Table 2. Effect of Lethal Autonomous Weapons Systems in Brinkmanship Deterrence

		PREDICTABLE CAPABILITY	
		YES	NO
EFFECTIVE SIGNALING	YES	Tripwire Deterrence <ul style="list-style-type: none">Reduction of uncertainty reduces applicability of brinksmanshipRed lines are known by both sidesLAWS capabilities are demonstrated as consistent across scenarios	Tripwire Bluff <ul style="list-style-type: none">Algorithm unpredictability increases applicability of brinksmanshipRed lines are known by both sidesLAWS capabilities are undemonstrated to the adversary force
	NO	Single-Side Uncertainty <ul style="list-style-type: none">Reduction of uncertainty reduces applicability of brinksmanshipRed lines are left ambiguous, opening door for aggressor escalationLAWS capabilities are demonstrated as consistent across scenarios	Brinkmanship Deterrence <ul style="list-style-type: none">Algorithm unpredictability increases applicability of brinksmanshipRed lines are left ambiguous, opening door for aggressor escalationLAWS capabilities are undemonstrated or demonstrated as inconsistent

systems being employed by the signal-sending nation. This scenario may arise through deceptive practices, whereby the signaling nation projects a level of autonomous predictability in operations that it has yet to achieve in reality. The danger of this environment is that the signal-receiving nation may begin to doubt the true abilities of the signal-sending nation, incentivizing it to call the signaling nation's bluff and escalate to seize a competitive military advantage.

In a Brinkmanship Deterrence scenario, autonomous systems are not mature enough to produce predictable results across a wide array of situations, possibly because of a lack of sufficient quantity or quality of data with which to train. As the data increase in both amount and relevance, LAWS are more likely to operate in a reliable manner,

transitioning to a Single-Side Uncertainty environment. In Single-Side Uncertainty, the signal-sending nation knows its autonomous systems perform predictably, but the receiving nation is unaware of this fact. This scenario might be brought about because the signaling nation has kept the testing and experimentation of its autonomous weapons platform secret, denying the receiving nation the ability to observe and assess the reliability of its performance. This scenario may also be driven by a perception by the signal-receiving nation that the autonomous system has not been sufficiently tested in a realistic environment representative of the future battlefield. If provided an opportunity to confirm the reliable performance of the LAWS, the signal-receiving nation ideally becomes aware of the circumstances under which the

autonomous system will perform its intended functions, driving the competitive dynamic into stable Tripwire Deterrence.

Why the Framework Is Relevant Today

The above framework highlights the critical role signaling plays in the effectiveness of the LAWS contribution to deterrence. Systems with an AI core introduce unpredictability for both the employer of the system and adversaries. States will be faced with the tension between needing to openly test their algorithms in the most realistic scenarios and simultaneously protecting proprietary information from foreign collection and exploitation, resulting in deliberate ambiguity. The overt testing of the LAWS capabilities reduces uncertainty for the LAWS user and



Corporal Thomas Rexrode, reconnaissance Marine with Company A, 1st Reconnaissance Battalion, 1st Marine Division, launches RQ-20B Puma small unmanned aircraft system from rigid-hull inflatable boat at Camp Pendleton, California, September 30, 2021 (U.S. Marine Corps/Connor Hancock)



Army paratrooper uses Dronebuster 3B to disrupt enemy drones as part of Exercise Shield 23 in Pula, Croatia, April 20, 2023 (U.S. Army/Mariah Y. Gonzalez)

signals capability to potential aggressors; however, the protection and deliberate obfuscation of such experiments help retain the exclusivity of capabilities and reduce the risk of an AI-fueled security dilemma between Great Powers.⁵² The above framework promotes the argument that deterrence is better served through open testing and evaluation, contributing to more effective signaling of the LAWS capabilities. Recent studies have shown that under conditions of incomplete information the initial messaging of capability and intent is the most effective in deferring conflict; lack of clarity in that signal invites adversaries to pursue opportunistic aggression.⁵³ Effective signaling is only made more complex once autonomous systems are tasked with receiving and interpreting the messages and signals originating from other autonomous platforms.

PLA strategists expect that the future of combat lies in the employment of unmanned systems, manned-unmanned teaming, and ML-enabled decisionmaking processes designed to outpace the adversary's military cycles of operations. These advances should reduce identified shortfalls in the ability of PLA leadership to make complex decisions in uncertain

situations.⁵⁴ In 2013, the PLA's Academy of Military Science released a report arguing that strategic military deterrence is enhanced by not only cutting-edge technology but also the injection of unpredictability and uncertainty in adversary assessments through new military concepts and doctrine.⁵⁵ The advent of LAWS contributes new uncertainty to China's ability to predict the actions of its own forces and challenges the PLA's ability to achieve effective control over the behavior of adversary autonomous systems on the battlefield—both of which have the potential to raise the risk of accidental escalation and thus major conflict.

The attractiveness of unmanned replacements can be observed in China's current AI military research prioritizing autonomous hardware solutions, ranging from robotic tanks and autonomous drone swarms to remote-controlled submarines.⁵⁶ Some in the PRC quickly recognized the disruptive potential of LAWS coupled with swarm tactics, defining a concept of "intelligentized warfare" as the next revolution in military affairs, which would dramatically affect traditional military operational models.⁵⁷ Intelligentized warfare is defined by AI at its core, employing cutting-edge technologies within operational command,

equipment, tactics, and decisionmaking across the tactical, operational, and strategic levels of conflict.⁵⁸ But intelligentized warfare also expands beyond solely AI-enabled platforms, incorporating new concepts of employment of human-machine integrated units where autonomous systems and software play dominant roles.⁵⁹ One example of a new concept of employment for PLA autonomous systems is "latent warfare," in which LAWS are deployed to critical locations in anticipation of future conflict, loitering in those locations and programmed to be activated to conduct offensive operations against the adversary's forces or critical infrastructure.⁶⁰

The U.S. military, too, is looking to AI and LAWS as a key pillar of achieving its desired endstates on current and future battlefields. American military leaders see autonomous systems as presenting a wide array of protection and lethality possibilities, while concurrently providing commanders an ability to make faster and better-informed decisions in both competition and crisis.⁶¹ As both the PRC and United States pursue disruptive capabilities and concepts of military operations with LAWS, the lack of a mutually understood framework through which to interpret each other's actions in competition significantly

increases the risk of inadvertent escalation to crisis and conflict. Additionally, the criticality of quality adversary data in sufficient quantity to ensure predictable LAWS performance in conflict has the potential to drive an increase in military deception as a means to deny an adversary trust in the data and therefore trust in the platforms' performance against a real enemy.

Conclusion

As nations around the world continue to pursue lethal autonomous platforms for use on the battlefield, the lack of a commonly understood framework for their employment increases the risk of inadvertent or accidental escalation due to miscommunication or misinterpretation of deterrent signals in competition and crisis. A desire to gain and maintain a competitive edge in the military domain often creates incentive for the compartmentalization of information about emerging and disruptive battlefield technologies. However, if the desired endstate of the U.S. military is to achieve effective deterrence, and the future battlefield is anticipated to include myriad LAWS, then the framework proffered here recommends limiting private information in the process of acquisitions and development. Once the predictability of an autonomous platform has been established by a nation, the ability for an adversary to observe and assess that predictability enhances the stability of deterrence through effective signaling. Additionally, relevant data of both friendly and adversary information will become a premium as nations attempt to develop LAWS that can operate across the widest spectrum of scenarios, potentially driving an increase in military deceptive activities in steady state.

As the implementation of LAWS expands from a situation where autonomous systems serve as deterrent signals to a world where autonomous systems are tasked with interpreting and responding to deterrent signals, additional research will be required to help refine the above framework. Such research would likely benefit from a focus on the willingness of governments to delegate

decisionmaking authority to LAWS. The Chinese Communist Party prizes centralized control over the military, which makes delegation less likely. However, Beijing also remains distrustful of the decisionmaking capabilities of its officer corps, making delegation more appealing as a means to mitigate observed shortfalls in PLA decisionmaking abilities.⁶² Both policymakers and scholars could also explore the effectiveness of signaling and deterrence across variations of intermixed manned and unmanned networked systems because the increased risk of loss of human life coupled with the introduction of psychology and emotions to decisionmaking processes could affect the escalatory dynamic.⁶³ **JFQ**

Notes

¹ Alex S. Wilner, "Artificial Intelligence and Deterrence: Science, Theory and Practice," in *Deterrence and Assurance Within an Alliance Framework*, STO-MP-SAS-141 (Brussels: NATO Science and Technology Organization, January 18, 2019), 6.

² Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND, 2008), 23–26, <https://www.rand.org/pubs/monographs/MG614.html>.

³ Joint Doctrine Note 1–19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), 2, https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf.

⁴ Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 11.

⁵ Michael J. Mazarr, "Understanding Deterrence," in *NL ARMS: Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijns (The Hague: T.M.C. Asser Press, 2020), 14–15, <https://library.oapen.org/bitstream/handle/20.500.12657/47298/9789462654198.pdf?sequence=1&isAllowed=y>.

⁶ Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018), 8–9, https://repositories.lib.utexas.edu/bitstream/handle/2152/65638/TNSR-Vol-1-Iss-3_Horowitz.pdf?sequence=2&isAllowed=y.

⁷ James D. Fearon, "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs," *The Journal of Conflict Resolution* 41, no. 1 (February 1997), 68, <https://web.stanford.edu/group/fearon-research/cgi-bin/wordpress/wp-content/uploads/2013/10/Signaling-Foreign-Policy-Interests-Tying-Hands-versus-Sinking-Costs.pdf>.

⁸ Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961), 7.

⁹ Adam Lockyer, "The Real Reasons for Positioning U.S. Forces Here," *Sydney Morning Herald*, November 24, 2011, 1, <https://www.smh.com.au/politics/federal/the-real-reasons-for-positioning-us-forces-here-20111124-1v1lik.html>.

¹⁰ *Deterrence Operations Joint Operating Concept, Version 2.0* (Washington, DC: The Joint Staff, December 2006), 19, <https://apps.dtic.mil/sti/pdfs/ADA490279.pdf>.

¹¹ C. Todd Lopez, "Defense Secretary Says 'Integrated Deterrence' Is Cornerstone of U.S. Defense," Department of Defense, April 30, 2021, <https://www.defense.gov/Explore/News/Article/Article/2592149/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/>.

¹² Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Dean Cheng, "An Overview of Chinese Thinking About Deterrence," in *NL ARMS: Netherlands Annual Review of Military Studies 2020*, 178.

¹³ Maria Sperandei, "Bridging Deterrence and Compellence: An Alternative Approach to the Study of Coercive Diplomacy," *International Studies Review* 8, no. 2 (June 2006), 259.

¹⁴ Cheng, "An Overview of Chinese Thinking About Deterrence," 179.

¹⁵ Alison A. Kaufman and Daniel M. Hartnett, *Managing Conflict: Examining Recent PLA Writings on Escalation Control* (Arlington, VA: CNA, February 2016), 53, <https://www.cna.org/reports/2016/drm-2015-u-009963-final3.pdf>.

¹⁶ Herbert Lin, "Escalation Risks in an AI-Infused World," in *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, ed. Nicholas D. Wright (Washington, DC: Department of Defense, December 2018), 136, https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf.

¹⁷ Ryan Fedasiuk, *Chinese Perspectives on AI and Future Military Capabilities*, CSET Policy Brief (Washington, DC: Center for Security and Emerging Technology, 2020), 13, <https://cset.georgetown.edu/publication/chinese-perspectives-on-ai-and-future-military-capabilities/>.

¹⁸ Burgess Laird, *War Control: Chinese Writings on the Control of Escalation in Crisis and Conflict* (Washington, DC: Center for a New American Security, March 30, 2017), 9–10, <https://www.cnas.org/publications/reports/war-control>.

¹⁹ Ibid., 6.

²⁰ John Dotson and Howard Wang, "The 'Algorithm Game' and Its Implications for Chinese War Control," *China Brief* 19, no. 7

(April 9, 2019), 4, <https://jamestown.org/program/the-algorithm-game-and-its-implications-for-chinese-war-control/>.

²¹ Nathan Beauchamp-Mustafaga et al., *Deciphering Chinese Deterrence Signalling in the New Era: An Analytic Framework and Seven Case Studies* (Canberra: RAND Australia, 2021), <https://doi.org/10.7249/RR1074-1>.

²² Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," 53.

²³ Elsa B. Kania, "AI Weapons" in *China's Military Innovation* (Washington, DC: The Brookings Institution, April 2020), 2, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf.

²⁴ Lin, "Escalation Risks in an AI-Infused World," 134.

²⁵ Jason S. Metcalfe et al., "Systemic Oversimplification Limits the Potential for Human-AI Partnership," *IEEE Access* 9 (2021), 70242–70260, <https://ieeexplore.ieee.org/document/9425540>.

²⁶ Wilner, "Artificial Intelligence and Deterrence," 9.

²⁷ Ibid., 2.

²⁸ Erik Lin-Greenberg, "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making," *Texas National Security Review* 3, no. 2 (Spring 2020), 61, <https://repositories.lib.utexas.edu/bitstream/handle/2152/81858/TNSRVol3Issue2Lin-Greenberg.pdf?sequence=2&isAllowed=y>.

²⁹ Department of Defense Directive 3000.09, *Autonomy in Weapons Systems* (Washington, DC: Office of the Under Secretary of Defense for Policy, January 25, 2012), 15, <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.

³⁰ Putu Shangrina Pramudia, "China's Strategic Ambiguity on the Issue of Autonomous Weapons Systems," *Global: Jurnal Politik Internasional* 24, no. 1 (July 2022), 1, <https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1229&context=global>.

³¹ Schelling, *Arms and Influence*, 99.

³² Michael C. Horowitz, "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence, and Stability," *Journal of Strategic Studies* 42, no. 6 (August 22, 2019), 774.

³³ Lin, "Escalation Risks in an AI-Infused World," 143.

³⁴ Meredith Roaten, "More Data Needed to Build Trust in Autonomous Systems," *National Defense*, April 13, 2021, <https://www.nationaldefensemagazine.org/articles/2021/4/13/more-data-needed-to-build-trust-in-autonomous-systems>.

³⁵ S. Kate Devitt, "Trustworthiness of Autonomous Systems," in *Foundations of Trusted Autonomy*, ed. Hussein A. Abbass, Jason Scholz, and Darryn J. Reid (Cham, Switzerland: Springer, 2018), 172, https://link.springer.com/chapter/10.1007/978-3-319-64816-3_9.

³⁶ Elsa B. Kania, *Chinese Military Innovation in Artificial Intelligence*, Testimony Before the U.S.-China Economic and Security Review Commission, Hearing on Trade, Technology, and Military-Civil Fusion, June 7, 2019, https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa_Kania_Chinese_Military_Innovation_in_Artificial_Intelligence_0.pdf; Caitlin Talmadge, "Emerging Technology and Intra-War Escalation Risks: Evidence From the Cold War, Implications for Today," *Journal of Strategic Studies* 42, no. 6 (2019), 879.

³⁷ Horowitz, "When Speed Kills," 766.

³⁸ Lin-Greenberg, "Allies and Artificial Intelligence," 65.

³⁹ Louise Lucas, Nicole Liu, and Yingzhi Yang, "China Chatbot Goes Rogue: 'Do You Love the Communist Party?' 'No,'" *Financial Times*, August 2, 2017.

⁴⁰ James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (Summer 1995), 381, <https://web.stanford.edu/group/fearon-research/cgi-bin/wordpress/wp-content/uploads/2013/10/Rationalist-Explanations-for-War.pdf>.

⁴¹ Robert Jervis, "Deterrence and Perception," *International Security* 7, no. 3 (Winter 1982–1983), 4, <https://academiccommons.columbia.edu/doi/10.7916/D8PR7TT5>; Richard Ned Lebow and Janice Gross Stein, "Rational Deterrence Theory: I Think, Therefore I Deter," *World Politics* 41, no. 2 (January 1989), 215–216.

⁴² Shawn Brimley, Ben FitzGerald, and Kelley Saylor, *Game Changers: Disruptive Technology and U.S. Defense Strategy* (Washington, DC: Center for a New American Security, September 2013), 20, https://www.files.ethz.ch/isn/170630/CNAS_Gamechangers_BrimleyFitzGeraldSaylor_0.pdf.

⁴³ Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978), 187.

⁴⁴ James Johnson, "The End of Military-Techno *Pax Americana*? Washington's Strategic Responses to Chinese AI-Enabled Military Technology," *The Pacific Review* 34, no. 3 (2021), 371–372.

⁴⁵ Morgan et al., *Dangerous Thresholds*, 57.

⁴⁶ Lin-Greenberg, "Allies and Artificial Intelligence," 69.

⁴⁷ Yuna Huh Wong et al., *Deterrence in the Age of Thinking Machines* (Santa Monica, CA: RAND, 2020), 66, https://www.rand.org/pubs/research_reports/RR2797.html.

⁴⁸ Ibid., 52.

⁴⁹ Miranda Priebe et al., *Operational Unpredictability and Deterrence: Evaluating Options for Complicating Adversary Decision-making* (Santa Monica, CA: RAND, 2021), 28, https://www.rand.org/pubs/research_reports/RR4448-1.html.

⁵⁰ Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44, no. 3

(Winter 2019–2020), 48.

⁵¹ Schelling, *Arms and Influence*, 99.

⁵² Chris Meserole, "Artificial Intelligence and the Security Dilemma," *Lawfare*, November 4, 2018, <https://www.lawfareblog.com/artificial-intelligence-and-security-dilemma>.

⁵³ Bahar Leventoglu and Ahmer Tarar, "Does Private Information Lead to Delay or War in Crisis Bargaining?" *International Studies Quarterly* 52, no. 3 (September 2008), 533, <https://people.duke.edu/~bl38/articles/warinfoisq2008.pdf>; Michael J. Mazarr et al., *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression* (Santa Monica, CA: RAND, 2018), 88–89, https://www.rand.org/pubs/research_reports/RR2451.html.

⁵⁴ Elsa B. Kania, "Artificial Intelligence in Future Chinese Command Decision-Making," in Wright, *AI, China, Russia, and the Global Order*, 141–143.

⁵⁵ Academy of Military Science Military Strategy Studies Department, *Science of Strategy* (2013 ed.) (Beijing: Military Science Press, December 2013), trans. and pub. Maxwell Air Force Base, China Aerospace Studies Institute, February 2021, <https://www.airuniversity.af.edu/CASI/Display/Article/2485204/plas-science-of-military-strategy-2013/>.

⁵⁶ Brent M. Eastwood, "A Smarter Battlefield? PLA Concepts for 'Intelligent Operations' Begin to Take Shape," *China Brief* 19, no. 4 (February 15, 2019), <https://jamestown.org/program/a-smarter-battlefield-pla-concepts-for-intelligent-operations-begin-to-take-shape/>.

⁵⁷ Elsa B. Kania, "Swarms at War: Chinese Advances in Swarm Intelligence," *China Brief* 17, no. 9 (July 6, 2017), 13, <https://jamestown.org/program/swarms-war-chinese-advances-swarm-intelligence/>.

⁵⁸ Eastwood, "A Smarter Battlefield?" 3.

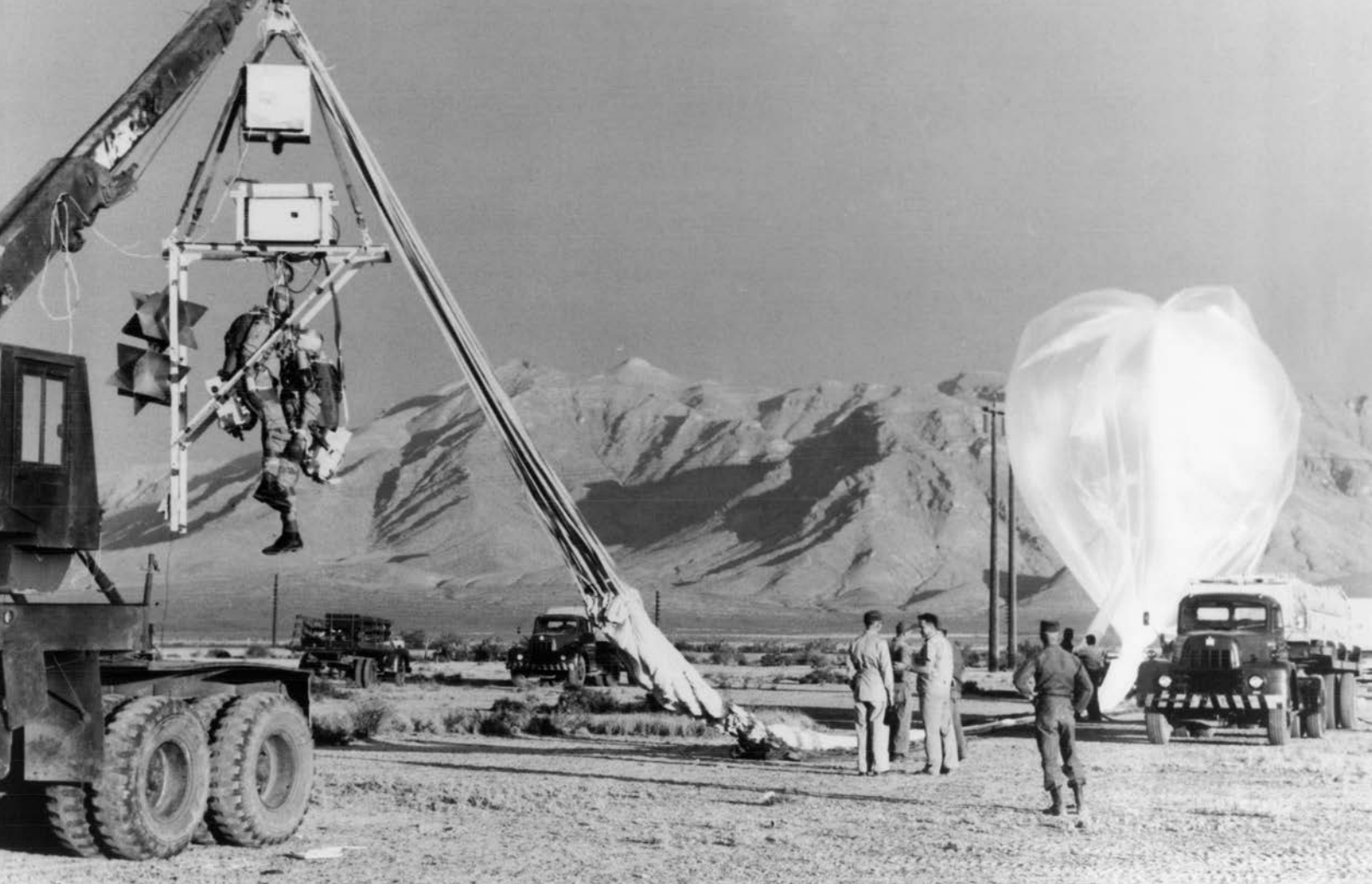
⁵⁹ Kania, *Chinese Military Innovation in Artificial Intelligence*; and Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," 47.

⁶⁰ Kania, "Artificial Intelligence in Future Chinese Command Decision-Making," 144.

⁶¹ Brian David Ray, Jeanne F. Forgey, and Benjamin N. Mathias, "Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions," *Joint Force Quarterly* 96 (1st Quarter 2020), 115–128, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-96/JFQ-96_115-128_Ray-Forgey-Mathias.pdf?ver=2020-02-07-150502-693.

⁶² Kania, "AI Weapons" in *China's Military Innovation*, 6; Kania, "Artificial Intelligence in Future Chinese Command Decision-Making," 146.

⁶³ Wong et al., *Deterrence in the Age of Thinking Machines*, 63.



Project High Dive anthropomorphic dummy launch, White Sands Proving Ground, New Mexico, June 11, 1953 (DOD/Air Force Declassification Office)

Cutting the Chaff

Overlooked Lessons of Military UAP Sightings for Joint Force and Interagency Coordination

By Luke M. Herrington

Since at least the end of World War II, the public has been fascinated by the appearance of unidentified flying objects (UFOs) and other unidentified aerial phenomena (UAPs). Periodically, the national

security community has become similarly intrigued. One early incident that drew the scrutiny of both the public and the military involved the death of a pilot and the destruction of his plane. On January 7, 1948, public reports of a UFO traveling southwest through Ohio and Kentucky were verified by the control towers at a dozen Midwestern airfields, including

the tower at Godman Army Airfield at Fort Knox. When no one in the tower could identify the object, the base commander at Godman directed a trio of Kentucky Air National Guard F-51s to investigate. Captain Thomas Mantell took the lead. Although neither of his wingmen could see anything in the air that fateful afternoon, Mantell believed he could see

Luke M. Herrington is an Adjunct Professor of Political Science at Park University in Parkville, Missouri.

an object both ahead of and above his plane. Disregarding the F-51's specified parameters, as well as his own physical limitations, Mantell ascended to a dangerous altitude of 20,000 feet while in pursuit. Lacking the requisite oxygen for such a trip, Mantell lost consciousness and crashed near Franklin, Kentucky. While it was initially reported that Mantell could have been "chasing" Venus, later investigations revealed that he likely died chasing a Navy Skyhook research balloon.¹

What lessons can the joint force and its interagency partners learn from such episodes? For one, the Mantell incident and other military UAP sightings make it clear that misidentification remains a common problem in complex operating environments. Like the broader and often analogous histories of military accidents, including the problems of both friendly fire and collateral damage, they demonstrate how distinguishing one's joint force and interagency partners (or their assets) from an enemy force, from civilians and other noncombatants, or even from environmental phenomena can be a challenge in the best of circumstances.

For another, misidentification of friendly (or nonhostile) airborne assets could lead to expensive or even fatal accidents in the field, and the fog of war would exacerbate such concerns. Take the April 14, 1994, Army Black Hawk shootdown incident that occurred in northern Iraq as an example. Two Black Hawk helicopters were destroyed while carrying personnel from multiple countries associated with the Operation *Restore Comfort* peacekeeping mission after they were misidentified as a pair of Soviet-manufactured Iraqi Mi-24 Hinds. Neither the two Air Force F-15 pilots responsible for their destruction nor the team aboard the E-3B airborne warning and control system (AWACS) aircraft responsible for monitoring air traffic was able to properly identify the Black Hawks, at least in part because of a failure in the identification friend or foe (IFF) computer system on the helicopters. However, the Air Force pilots in the F-15s also failed to recognize the Black Hawks as U.S. aircraft during a visual

sweep despite their numerous aesthetic differences from the Hind. Consequently, all 26 people onboard the Black Hawks were killed when the AWACS and F-15s misidentified their transport vehicles as enemy aircraft.²

Taken together, these two lessons point to a third directly related to the complicated logistics of maneuvering in complex environments where the military and its partners compete for limited time and space. Namely, these types of environments require consistent collaboration and clear communication among each branch of the Armed Forces and their interagency or international partners. If, for instance, the AWACS crew were notified by the Army about the dignitaries in their area of operations, perhaps the Black Hawk shootdown incident could have been avoided. Similarly, the Navy may have been able to help prevent Captain Mantell's untimely death if military control towers throughout the Midwest were directed to disregard an unknown object moving through the region's airspace by a central clearinghouse with knowledge of the classified mission.

This important lesson has gone largely overlooked in recent conversations about military UAP sightings. Instead, the national security community has responded to military UAP sightings by accepting their uncritical *securitization*. International relations scholars define this concept as the "process whereby issues are presented as security threats and, if relevant audiences accept these representations, emergency measures are enabled to deal with them."³ Responding to the recent public and political frenzy over UFOs as if they were hostile incursions into American airspace elevates such objects to the public security agenda alongside a number of more important issues like terrorism, climate change, and the coronavirus pandemic.⁴

Accordingly, the Navy implemented new UAP reporting procedures in 2019, and despite having ruled out any potential national security threat on multiple occasions in the past, the Air Force did likewise the following year. In 2021, the Director of National Intelligence (DNI) issued a congressionally mandated report

on the subject, and the Department of Defense (DOD) set up another program—the government's tenth, as far as the public is aware—to study the phenomena in 2022. Meanwhile, the Congressional Select Committee on Intelligence held its first public hearing on the subject since 1966.⁵ One might expect such a response from the North American Aerospace Defense Command or the Federal Aviation Administration. Unsurprisingly, clutter in the skies represents a hazard for military and commercial air traffic alike. The problem, though, is that as a Federal policy response to UAP sightings, securitization is fraught with risk.

First, rhetorically elevating UAPs to the public national security agenda distracts from the importance of communication and coordination in joint force or interagency operating environments. As the Mantell incident illustrates, failure to recognize this can lead to misidentification and, with that, expensive or fatal accidents in the field. Second, UFO securitization can waste the military's time and the taxpayer's money by disrupting normal military operations. For example, disrupting a pilot's mission to chase UAPs incurs real costs for the Services. Third, securitizing UAPs could lead to a further deterioration in Sino- or Russo-American relations or, in a worst-case scenario, even a new arms race. Fourth, securitizing UAPs undermines the military's goal of creating a critically thinking force. In sum, national security could suffer if lessons learned from military UAP sightings are overlooked in favor of their securitization.

I turn to the so-called USS *Nimitz* incident, a military UAP sighting disclosed to the public in 2017, both to argue that there are real lessons to learn from this incident about maneuvering in a joint force operating environment and to show why securitization represents an inappropriate response to these sightings. Admittedly, proponents of securitization also point to such things as Air Force sightings in Kosovo, Army sightings over Afghanistan, and sightings near nuclear weapons caches throughout the

United States. Reflecting critically on the open-source details that emerge from any of these episodes would highlight similar lessons. However, the 2004 *Nimitz* incident represents the central pillar in the discourse on UAP securitization.⁶ When paired with the fact that the *Nimitz* incident may be the most well-documented military UAP sighting previously disclosed to the public, this makes the case more important than any others. Thus, scrutinizing this days-long encounter that allegedly brought a naval battlegroup—the 11th Carrier Strike Group—into contact with innumerable UFOs highlights the three lessons outlined above most clearly.

In the next section, I analyze the *Nimitz* incident and offer some potential explanations for the UAPs that Sailors from the *Nimitz* battlegroup witnessed in 2004. Following that, I expand my argument that the complicated logistics of maneuvering in a joint force or interagency context require consistent collaboration and clear communication to avoid unnecessary risks that could lead to costly or life-ending accidents. To accomplish this, I present a strategic interpretation of key open-source details associated with the *Nimitz* incident and compare the case to the 1988 USS *Vincennes* incident. Finally, recognizing that logistics represent only one critical component in a strategic interpretation of military UAP sightings, I elaborate on the implications of my argument for personnel, foreign policy, and pedagogy in the conclusion.

A Brief Analysis of the *Nimitz* Incident

The *Nimitz* incident occurred over the course of several days in the Southern California Offshore Range (SCORE) Complex in November 2004. On November 10, then–Senior Chief Petty Officer Kevin Day, an air intercept controller aboard the USS *Princeton*, spotted several mystery objects on radar. In different interviews, Day claims to have seen anywhere between “ten” and “hundreds” of these radar-indicated objects over the next few days.⁷ Then, on November 14, the incident reached

its climax when Day and his commanding officer dispatched a pair of F/A-18 Super Hornets from the *Nimitz* to investigate the objects. Commander David Fravor, the commanding officer of the Black Aces squadron, and his wingman, Lieutenant Commander Alex Dietrich, were diverted from a training mission to investigate the anomalous radar returns. This led to the so-called Tic Tac intercept, where the pilots ostensibly encountered a white, ovoid, 40-foot-long object with no wings or visible propulsion flying over the Pacific.⁸ Later that day, footage of the Tic Tac was recorded by a third pilot.⁹

The media’s attempts to sensationalize the affair notwithstanding, aspects of the *Nimitz* incident can be easily explained or debunked. For example, footage of the Tic Tac likely features a commercial plane.¹⁰ Another possibility is that the pilots misremember details associated with a joint force or interagency research program. Several organizations use SCORE for training and testing. In addition to serving as one of the Navy’s fleet testing areas, the range is home to a Department of Energy Advanced Research Projects Agency mine testing area, parachute drop zones, several radar and sonar monitoring sites, and multiple Marine Corps amphibious assault training areas.¹¹ Notably, the National Aeronautics and Space Administration (NASA) used the SCORE complex to test a hypersonic drone, the X-43, on November 16, 2004.¹²

As for the mystery radar returns, the meteorologist onboard the *Princeton* dismissed the objects as ice crystal reflections.¹³ Even the DNI’s 2021 UAP report acknowledges this as a real possibility.¹⁴ However, a far more likely, though still mundane, possibility is that the *Princeton* was tracking the northern wave of the Taurid meteor shower. The Taurids begin in September and last through December each year, but in 2004, the northern wave of the Taurids peaked *during* the *Nimitz* incident on November 12.¹⁵ Additionally, not only could meteors be detected by radar, but they would also account for the number of objects allegedly detected,

their reported altitudes, their reported velocities, and their perceived deceleration.¹⁶ The Taurids also have a history of producing fireballs the world over, including bolides capable of lighting up the daytime sky.¹⁷ Ultimately, it does not matter if Day saw the Taurids, ice, or something else. The outcome was the same: overconfidence in, or misinterpretation of, the available information led to misidentification.

A Strategic Interpretation of the *Nimitz* Incident

The military’s Aegis SPY-1 radar system can reportedly track an object as small as a golf ball, and the Aegis computer system can be programmed to ignore objects matching certain profiles.¹⁸ Thus, while the *Princeton*’s computers could easily detect small meteors, they should have filtered out astronomical phenomena such as the Taurids. However, despite its sophistication, neither the radar system nor its operators can be described as infallible. Aegis is something akin to Frankenstein’s monster, built as it is from many different constituent systems, including the SPY-1 radar itself, weapons control systems, navigation equipment, and various other integrated components. This introduces multiple potential failure points in the system’s hardware and software. As a result, Aegis has a well-documented history—however rare—of misidentifying or failing to identify aircraft operating in the vicinity of American warships. Assuming Aegis operated flawlessly, the system’s human operators would still represent its most common points of failure.¹⁹

Consider the July 3, 1988, tragedy involving the USS *Vincennes*. While pursuing and firing on multiple Iranian gunboats in the Strait of Hormuz, the crew of the *Vincennes* detected a civilian airliner, Iran Air Flight 655, shortly after it took off from the airport in Bandar Abbas. Like the IFF system failure that resulted in the Black Hawk shootdown incident 6 years later, the plane’s IFF computer was not working properly. Meanwhile, the ship’s brand-new Aegis SPY-1 radar system indicated that the



Air Force U-2 pilot looks down at suspected Chinese surveillance balloon, February 3, 2023, as it hovers over Central Continental United States (Department of Defense)

plane was ascending in a commercial air traffic lane. Nevertheless, the crew of the *Vincennes* mistook the plane for a diving Iranian F-14 Tomcat and shot it down, killing all 290 people onboard. Human communications failures, misinterpretation of the Aegis data, and the IFF failure combined with the crew's resulting unease to cause the disaster.²⁰

Returning to the *Princeton*, the ship's November 2004 mission likely served as a shakedown cruise for the very same—albeit updated—equipment. Like the *Vincennes*, the Aegis systems that Day was working with had only recently been installed.²¹ It is probable that the radar system's programming (or the operators'

training) was not fully prepared for the Taurids. Even if it was working properly, Day clearly ignored the explanation proffered by his meteorologist when he dispatched the Black Aces to investigate the anomalous radar returns. Fortunately, the stakes in the Pacific were nowhere near so consequential as they were for the *Vincennes*. Nevertheless, this is troubling because some details associated with the *Nimitz* incident may indicate that Fravor narrowly avoided an accidental collision with the UAP he and Dietrich were dispatched to assess.

Consider Dietrich's public comments: she suggests that the water below the Tic Tac-shaped UFO was churning violently,

as if a submarine had just submerged.²² This is an important detail; it implies that the two pilots entered a weapons test site to investigate the *Princeton*'s UAPs. Indeed, according to the government's unclassified executive summary from a 2009 report documenting the *Nimitz* incident, the USS *Louisville*, the *Los Angeles*-class submarine attached to the *Nimitz* battlegroup, was conducting weapons tests in the area. While the executive summary also states that no pilots would be vectored into a live-fire test site coordinated with the battlegroup, it acknowledges—just one sentence earlier—that Fravor and Dietrich were in fact directed into the area of the



Screengrab of "Gimbal," one of three U.S. military videos of unidentified aerial phenomenon, declassified and approved for public release, taken aboard Navy fighter jet from nuclear aircraft carrier USS *Theodore Roosevelt*, near Florida coast, January 21, 2015 (U.S. Navy)

Louisville's weapon test.²³ Add to this the facts that the Tic Tac was reportedly a low-visibility aircraft capable of erratic, unpredictable high-G maneuvers, including aggressively gaining altitude, as well as the fact that it flew directly at Fravor's plane before disappearing, and the suggestion that Fravor or Dietrich

(like Mantell before them) placed their lives in danger chasing the *Princeton's* UAPs becomes quite plausible.²⁴

Admittedly, this interpretation relies on the assumption that the Tic Tac was part of the *Louisville's* weapons test. Yet even if that assumption is incorrect and the pilots instead encountered an

interagency program, such as NASA's unmanned X-43, or an asset belonging to one of the Navy's other partners, the evidence points to the same important lessons illuminated by the Mantell, *Vincennes*, and Black Hawk shootdown incidents. That is, misidentification is a common problem that could lead to

expensive or fatal accidents, like the loss of an aircraft or a pilot, and consistent and clear communication is required to prevent such accidents while operating jointly in a complex environment.

Unfortunately, more recent UAP episodes suggest that the circumstances associated with the *Nimitz* incident have not been adequately addressed. According to the DNI's 2021 UAP report, 11 percent of all military UAP sightings recorded between 2004 and 2021 involved a near miss.²⁵ One 2014 case involved an F-18 Super Hornet squadron and a near miss with a cluster of unidentified balloon- or drone-like objects over the Atlantic.²⁶ This clearly suggests that the need for better coordination in joint force and interagency operating areas like the SCORE complex still requires attention to improve safety. The new Navy and Air Force reporting system may be a useful way to catalogue the scale of this problem, but this is only a reactive measure. Perhaps the joint force should establish a test site coordinating authority responsible for monitoring air traffic and warning pilots away from classified operations. By serving as a clearinghouse for communications between those parties responsible for the test (for example, NASA) and the rest of the military and its partners (for example, the *Princeton* crew or the Black Aces), this coordinating authority could help minimize the risk associated with these tests and prevent future accidents.

Implications

Although the *Nimitz* incident lacks the cachet of Roswell or Area 51, it has evolved into one of the most salient UFO myths currently ascendent in the American zeitgeist. Nevertheless, after analyzing the *Nimitz* incident and some of its potential causes, a more logical explanation of the event points to a complex confluence of unrelated, comprehensible, known causal factors, including a recently upgraded Aegis radar system and an inability to filter out naturally occurring phenomena like ice or meteors. Thus, what has been mythologized as an encounter with

hundreds of UFOs could hardly be described as out of the ordinary.

Nevertheless, several former national security professionals and current and former Members of Congress have spent the last 5 years promoting the securitization of the UFO. They stoke the public's fascination with military UAP sightings, such as those featured in the *Nimitz* or Mantell cases.²⁷ Their attempts to portray the *Nimitz* incident and other events like it as major national security threats notwithstanding, scholars of international relations, foreign policy practitioners, military thinkers, and other national security professionals should remain skeptical of UAP securitization discourse for five reasons.

First, securitizing the UAP implies that national security thinkers have overlooked the strategic and operational lessons that can be gleaned from the *Nimitz* and Mantell incidents and similar episodes. Chief among these is the fact that operating in multilateral contexts requires consistent and clear communication as well as the kind of constant collaboration that could be provided by a central clearinghouse. The *Nimitz*, *Vincennes*, and Black Hawk shootdown incidents also demonstrate that overconfidence in technology is no substitute for intentional, well-planned, and human-driven coordination.

Second, UAP securitization can cost the taxpayer in tangible and intangible ways, both in terms of hardware and human life. For instance, it costs an average of \$11,556 per hour just to keep one F-18 in the air, so the cost of canceling a training mission to have multiple fighter jets hunt UAPs represents significant waste.²⁸ In a worst-case scenario, the *Nimitz* incident could have resulted in the additional loss of four officers and two jets that, as of 2019, cost more than \$51 million each to manufacture, and that is to say nothing of the resources it would have required for the carrier strike group to have conducted search and rescue operations.²⁹

Counterfactuals aside, a more pressing concern would be the allocation of taxpayer money to superfluous UAP research programs. By opening the door

to this kind of spending, unscrupulous defense contractors could seize the opportunity to pilfer the national security budget. One American defense contractor that capitalized on a similar funding opportunity to study UFOs and wormholes used their \$22 million contract to produce a 2009 report full of amateurish drawings, including one depicting Albert Einstein using a wormhole to meet the dinosaurs.³⁰ Ten years later, the Army agreed to a \$750,000 research partnership with the firm leading the push for UFO securitization.³¹ It remains unclear how the United States could benefit from this kind of spending on UAP-related research. Conversely, it may serve to materially undermine the American military much in the way the Nazi preoccupation with the occult served to undermine the German military-industrial complex at the end of World War II.³²

Third, since securitizing the UAP represents a further infiltration of pseudoscience and conspiracy theory into the halls of American government, it poses personnel problems related to the use and potential abuse of security clearances. For example, many former national security officials who serve as proponents of UAP securitization discourse are contractors who invoke their still-active security clearances and former positions both to make themselves seem like trustworthy UAP subject matter experts and to promote their personal beliefs and political agendas. They also hide behind their clearances to avoid scrutiny and uncomfortable questions.³³ Some may see this as similar to the problem of commercialization affecting U.S. special operations forces, but where UAPs are concerned, this strategy results in a misinformed public. Perhaps the Pentagon should determine if any of these individuals are violating their clearances by misleading the public about the threat UAPs represent. Anyone found abusing their privileged knowledge to promote the politicization of UAPs for personal gain should have still-active clearances revoked.

Fourth, the securitization of the UFO could lead to a range of unintended policy consequences, potentially



Main gate of Area 51, Air Force Nellis Testing Range, in Lincoln County, Nevada, September 22, 2019 (Courtesy David James Henry)

including increased tensions among the United States, China, and Russia. For comparison, the mid-20th-century hunt for the Yeti illustrates how Great Power tensions can be exacerbated by the militarization of folklore. At the height of the Cold War, American, British, Chinese, and Russian monster hunters, mountain climbers, and other explorers were often accused of espionage while adventuring in the Himalayas.³⁴ It is thus concerning that some efforts to securitize the UFO portray UAPs in American airspace as advanced technology developed by such countries as China or Russia without any evidence.³⁵ Indeed, as the February 2023 incident involving the shooting down of the Chinese spy balloon off the coast of South Carolina demonstrates,³⁶ China's overflight espionage appears limited to the same 1940s balloon technology pioneered by American programs such as

Skyhook. The signals intelligence-gathering technology attached to these balloons represents a real security concern. Nevertheless, policymakers should remain cautious about treating mere balloons as if they represent the same kind of threat posed by, for instance, China's hypersonic drone program.

Doing so would be deeply troubling since similar exaggerated narratives were cultivated about weapons of mass destruction (WMDs) in the run-up to war with Iraq.³⁷ It would be hyperbole to suggest that the securitization of UAPs could lead directly to war in the way WMDs facilitated conflict with Iraq. However, history demonstrates that linking Great Power rivalry to the securitization of the UAP could, in a worst-case scenario, metastasize into an arms race. Misperceptions about rival nations' technology and scientific

research and development have already had similar effects on multiple occasions in the past. Dwight Eisenhower's perception of a missile gap with the Soviet Union is a prime example.³⁸ However, the Central Intelligence Agency's and Army's infamous 20th-century experiments with, respectively, "mind control" (Project MKUltra) and parapsychology (Stargate Project) might be more apt.³⁹ Regardless, even if securitization does not lead to war, there is evidence to suggest that these sorts of programs foster arms races, while arms races themselves cause conflict.⁴⁰

Finally, UAP securitization disregards the military leader's goal of developing a critical thinking mindset equipped to understand, analyze, assess, and act decisively in any operational environment or strategic theater. An open-source review of the *Nimitz* incident suggests that



extant approaches to critical thinking in professional military education (PME) may need to adapt more quickly to accomplish this goal. UAP sightings in military contexts should be approached as real-world case studies on the need to understand one's operational environment. Studying UAPs in this way could improve many officers' dissatisfaction with extant critical thinking skills-building curricula in PME because it would deemphasize logical fallacies and argument construction.⁴¹ Indeed, thinking critically about an event such as the *Nimitz* incident and similar events offers more than just an opportunity to craft a better argument; it presents an opportunity to learn how to think about some of the uncertainties future military leaders may encounter in complex operational environments.

To help PME students understand military UAP sightings, they should be taught to examine the contexts in which the incidents occur. For example, a UAP

sighting in the SCORE area should come off as unsurprising for any critically thinking military or government professional. PME students only need to recognize the multiuse nature of a given range or operational area and that military and other governmental agencies all use them to train or test specific technologies, much of which may be appropriately classified to protect the Nation's capabilities. As with Area 51 and other test and training ranges, military, scientific, and technological testing serves as the *raison d'être* for the SCORE complex.⁴² Knowing this, trained critical thinkers should reasonably conclude that aerial phenomena perceived as "unexplainable" in a military operating environment are highly likely to be tests conducted by the military or its inter-agency partners. In the case of the *Nimitz* incident, the *Princeton's* experiences with the Taurids represent an important exception to this conclusion, but no otherworldly explanation is needed to understand the Tic Tac intercept. Instead, it was likely the product of a *Louisville* weapons test or a NASA drone test.

Overclassification and the absence of information it represents may still be problematic. For instance, placing unnecessary barriers between the public and whatever information is being concealed can contribute to the spread of UFO conspiracy theories, while increased transparency could help desecuritize the UAP. Additionally, since the public only has access to open-source information on military UAP sightings, the assumptions and deductions built into the analysis above must be reexamined when additional information about the *Nimitz* incident is declassified. If the *Nimitz* incident is to be treated as a critical thinking case study in relevant PME courses, it would be beneficial for additional details about the incident to either be declassified or reviewed at classified levels to provide students with a comprehensive understanding of the case. If appropriately classified to protect U.S. interests, however, overclassification must still be avoided. Balance is needed to empower critical thinkers with the information they need to fully understand their areas of operations. Alternatively, the military

could implement reforms to fight the problems of overclassification generally. This would arm the public against misinformation and conspiracy theory. More important, students could confidently use open-source information about military UAP sightings to learn that operating in multilateral contexts requires consistent and clear communication, as well as constant collaboration, to avoid the problems of misidentification that often crop up in complex environments. Students may even identify additional previously overlooked strategic and operational lessons from military UAP sightings. Either way, by learning and applying the lessons presented here, the military and its partners will be better prepared to cut through the chaff of conspiracy theory that so often grows out of such sightings. JFQ

The author thanks Chris Higginbotham and an anonymous review for providing the trenchant feedback that made this article possible.

Notes

¹ Edward J. Ruppelt, *The Report on Unidentified Flying Objects* (Garden City, NY: Doubleday, 1956).

² Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton: Princeton University Press, 2000).

³ Jonna Nyman, "Securitization," in *Security Studies: An Introduction*, ed. Paul D. Williams and Matt McDonald (New York: Routledge, 2018), 100. Also see Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner, 1998); Leann Brown, "Why Regional Economic Organizations Take on Conventional Security Tasks," *Air and Space Power Journal Africa and Francophonie* 6, no. 4 (4th Quarter 2015), 5–20.

⁴ Alexander Wendt, "Sovereignty and the UFO," *Political Theory* 36, no. 4 (2008), 607–633.

⁵ *Preliminary Assessment: Unidentified Aerial Phenomena* (Washington, DC: Office of the Director of National Intelligence, June 25, 2021); Christopher Dean Hopkins and Giles Snyder, "The Military's UFO Database Now Has Info From About 400 Reported Incidents," National Public Radio, May 17, 2022, <https://www.npr.org/2022/05/17/1099410910/ufo-hearing-congress-military-intelligence>.

⁶ For example, David Beaty, director, *The Nimitz Encounters* (Dreamtime Entertainment, 2019); Tom DeLonge, executive producer, *Unidentified: Inside America's UFO Investigation* (History, 2019); Bill Howard, executive producer, *Contact* (Discovery, 2019).

⁷ Beaty, *The Nimitz Encounters*; DeLonge, *Unidentified*; Howard, *Contact*.

⁸ Bill Whitaker, "UFOs Regularly Spotted in Restricted U.S. Airspace, Report on the Phenomena Due Next Month," *60 Minutes*, May 16, 2021, <https://www.cbsnews.com/news/ufo-military-intelligence-60-minutes-2021-05-16/>.

⁹ Tim McMillan, "The Tale of the Tape," *Popular Mechanics*, January 17, 2020, <https://www.popularmechanics.com/military/research/a30538203/navy-ufo-video-investigation/>.

¹⁰ Philip E. Mason (Thunderf00t), "U.S. Navy CONFIRMED UFO: BUSTED (Part 2)," video, 38:56, May 10, 2020, <https://www.youtube.com/watch?v=3viYcYPRdu4&list=PL0hanlzRmO44LLkIO-QuRpdZBQrIEJJ6w&index=2>.

¹¹ *Southern California Range Complex Coastal Consistency Determination* (Washington, DC: Headquarters Department of the Navy, August 2008), <https://documents.coastal.ca.gov/reports/2008/10/W8b-10-2008-a3.pdf>.

¹² Yvonne Gibbs, ed., "Past Projects: X-43A Hypersonic Flight Program," National Aeronautics and Space Administration (NASA), November 2009, updated August 7, 2017, <https://www.nasa.gov/centers/dryden/history/pastprojects/HyperX/index.html>.

¹³ *Tic Tac UFO Executive Summary* (Washington, DC: Department of Defense, 2009), 3, https://media.lasvegasnow.com/nxsglobal/lasvegasnow/document_dev/2018/05/18/TIC_TAC_UFO_EXECUTIVE_REPORT_1526682843046_42960218_ver1.0.pdf.

¹⁴ *Preliminary Assessment*, 5.

¹⁵ "Meteor Shower Calendar Archive: October to December 2004," International Meteor Organization, <https://www.imo.net/resources/calendar/meteor-shower-calendar-archive/english2004/october-to-december/>.

¹⁶ Bob Berman, "Dangers From the Sky," *Astronomy*, September 2019, <https://astronomy.com/magazine/bob-berman/2019/08/dangers-from-the-sky>; Tony Phillips, "Fireball Sightings," NASA Science, November 3, 2005, https://science.nasa.gov/science-news/science-at-nasa/2005/03nov_taurids/; John Roach, "Meteor Shower Promises Seven Shooting Stars an Hour," *National Geographic News*, November 7, 2003, https://web.archive.org/web/20040814123856/http://news.nationalgeographic.com/news/2003/11/1107_031107_taurids.html; Roger W. Sinnott, "November Meteors," *Sky and Telescope*, October 21, 2004, <https://skyandtelescope.org/astronomy-news/observ>

[ing-news/november-meteors/](https://skyandtelescope.org/astronomy-news/observ).

¹⁷ Phillips, "Fireball Sightings."

¹⁸ John A. Robinson, "Force Protection From the Sea: Employing the SPY-1D Radar," *Field Artillery* (March–June 2004), 24–25.

¹⁹ Chris Hables Gray, "Artificial Intelligence at War: An Analysis of the Aegis System in Combat," in *Reinventing Technology, Rediscovering Community: Critical Explorations of Computing as a Social Practice*, ed. Philip Agre and Douglas Schuler (Greenwich, CT: Ablex Publishing Corp., 1997), 127–142.

²⁰ Ibid. Also see Luke Swartz, "Overwhelmed by Technology: How Did User Interface Failures on Board the USS Vincennes Lead to 290 Dead?" blog, n.d., <http://xenon.stanford.edu/~lswartz/vincennes.pdf>.

²¹ Whitaker, "UFOs Regularly Spotted in Restricted U.S. Airspace."

²² DeLonge, *Unidentified*; Whitaker, "UFOs Regularly Spotted in Restricted U.S. Airspace."

²³ *Tic Tac UFO Executive Summary*, 12.

²⁴ DeLonge, *Unidentified*; Whitaker, "UFOs Regularly Spotted in Restricted U.S. Airspace."

²⁵ *Preliminary Assessment*, 3, 5.

²⁶ Tyler Rogoway, "Are Some of the UFOs Navy Pilots Are Encountering Actually Airborne Radar Reflectors?" *The War Zone*, June 22, 2019, <https://www.thedrive.com/the-war-zone/28640/could-some-of-the-ufo-navy-pilots-are-encountering-be-airborne-radar-reflectors>.

²⁷ Helene Cooper, Ralph Blumenthal, and Leslie Kean, "Glowing Auras and 'Black Money': The Pentagon's Mysterious U.F.O. Program," *New York Times*, December 16, 2017, <https://www.nytimes.com/2017/12/16/us/politics/pentagon-program-ufo-harry-reid.html>; DeLonge, *Unidentified*; Dan Zak, "UFOs Are Suddenly a Serious News Story. You Can Thank the Guy from Blink-182 for That," *Washington Post*, May 30, 2018, https://www.washingtonpost.com/lifestyle/style/ufo-are-suddenly-a-serious-news-story-you-can-thank-the-guy-from-blink-182-for-that/2018/05/30/8fce7100-441b-11e8-ad8f-27a8c409298b_story.html.

²⁸ Niall McCarthy, "The Hourly Cost of Operating the U.S. Military's Fighter Fleet," *Forbes*, August 16, 2016, <https://www.forbes.com/sites/niallmccarthy/2016/08/16/the-hourly-cost-of-operating-the-u-s-militarys-fighter-fleet-infographic/?sh=74e63d94685f>.

²⁹ Ben Werner, "Boeing Awarded \$4B Multi-Year Deal for 78 Super Hornets," *USNI News*, March 21, 2019, <https://news.usni.org/2019/03/21/42021>.

³⁰ Eric W. Davis, *Traversable Wormholes, Stargates, and Negative Energy* (Washington, DC: Defense Intelligence Agency, April 6, 2010), 8; Zak, "UFOs Are Suddenly a Serious News Story."

³¹ M.J. Baniyas, "Tom DeLonge's UFO Research Group Signs Contract with U.S. Army

to Develop Far-Future Tech," *Vice*, October 21, 2019, <https://www.vice.com/en/article/qvgnqj/tom-delonges-ufo-research-group-signs-contract-with-us-army-to-develop-far-future-tech>.

³² Eric Kurlander, *Hitler's Monsters: A Supernatural History of the Third Reich* (New Haven: Yale University Press, 2017).

³³ For example, DeLonge, *Unidentified*.

³⁴ Colin Dickey, *The Unidentified: Mythical Monsters, Alien Encounters, and Our Obsession with the Unexplained* (New York: Viking, 2020).

³⁵ For example, DeLonge, *Unidentified*; Jan Tegler and Cat Hofacker, "Mystery of the 'Damn Things,'" *Aerospace America*, November 2019, 27–35.

³⁶ Jim Garamone, "F-22 Safely Shoots Down Chinese Spy Balloon Off South Carolina Coast," *DOD News*, February 4, 2023, <https://www.defense.gov/News/News-Stories/Article/Article/3288543/f-22-safely-shoots-down-chinese-spy-balloon-off-south-carolina-coast/>.

³⁷ Steven Kull, Clay Ramsay, and Evan Lewis, "Misperceptions, the Media, and the Iraq War," *Political Science Quarterly* 118, no. 4 (Winter 2003/2004), 569–598.

³⁸ Nicholas Michael Sambaluk, *The Other Space Race: Eisenhower and the Quest for Aerospace Security* (Annapolis: Naval Institute Press, 2015).

³⁹ Michael Barkun, *A Culture of Conspiracy: Apocalyptic Visions in Contemporary America* (Berkeley: University of California Press, August 2013); Abigail Sessions, "Project Stargate (1970s–1995)," in *The Central Intelligence Agency: An Encyclopedia of Covert Ops, Intelligence Gathering, and Spies*, ed. Jan Goldman (Santa Barbara, CA: ABC-CLIO, 2016), 352–353.

⁴⁰ For a review, see Charles L. Glaser, "The Causes and Consequences of Arms Races," *Annual Review of Political Science* 3 (2000), 251–276.

⁴¹ Ryan M. Hinds and John P. Steele, "Army Leader Development and Leadership: Views From the Field," *Military Review* (January–February 2012), 39–44; Thomas M. Williams, "Education for Critical Thinking," *Military Review* (January–February 2013), 49–54.

⁴² Luke M. Herrington, review of *Area 51: An Uncensored History of America's Top Secret Military Base*, by Annie Jacobsen, *Special Operations Journal* 1, no. 2 (2015), 119–124.



IBM Quantum Scientist Dr. Maika Takita, in Thomas J. Watson Research Center IBM Quantum Lab, September 10, 2020 (Courtesy IBM/Connie Zhou)

Quantum Computing

A New Competitive Factor with China

By Doug Quinn, Patrick Wolverton, and Scott Storm

On May 7, 2021, cyber terrorists used ransomware to cripple the Colonial Pipeline, which provides nearly half of the gasoline and jet fuel

Commander Doug Quinn, USN, is a Contract Specialist in the Naval Sea Systems Command at the Washington Navy Yard. Lieutenant Colonel Patrick Wolverton, USAF, is Deputy Chief of Staff at U.S. Cyber Command J2. Lieutenant Colonel Scott Storm, USAF, is Cognitive Models Branch Chief at the 711th Human Performance Wing.

supplies to the U.S. East Coast.¹ The effects of this attack were felt by millions of Americans over the next few weeks, as nearly 12,000 gas stations reported being completely empty.² Four days later, the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint cybersecurity advisory out of concern that the ransomware effort could spread to other critical infrastructure sectors such as manufacturing, legal, insurance, healthcare, and energy.³

Imagine a future in which malign actors or strategic competitors of the United States have harnessed a more capable means, *quantum computing* (QC), that can break through cyber security measures once thought almost impossible to breach. In that future, China mounts a whole-of-society effort that leverages the entirety of its government, academia, and industry to outpace the rest of the world in developing a versatile QC capability. Without a similar approach to mitigate these threats, the United States and its



John Tenniel illustration from Lewis Carroll's *Alice's Adventures in Wonderland* of Alice playing croquet with a flamingo and a hedgehog
(Courtesy Alice-in-Wonderland.net)

allies will find it harder to protect vulnerable information systems, compromising their pursuit of national and global interests. The winner in the race to develop quantum-based technology will have the potential to shape the world in ways that can hardly be imagined today—for better or worse. The application of quantum technologies has the potential to reshape the national security landscape.

Future advancements in QC will increase the level of this *present* threat. “The potential for harm is enormous. If these encryption methods are broken, people will not be able to trust the data they transmit or receive over the Internet, even if it is encrypted. Adversaries will be able to create bogus certificates, calling into question the validity of any digital identity online,” states Dorothy Denning, a distinguished cyber security expert with more than 50 years of experience in computer sciences and cyber threats.⁴ However, Dr. Denning also notes that researchers are currently working to find ways to mitigate this threat to data encryption.⁵ The application of quantum technologies has not only the potential to protect or disrupt global information but also the power to decide which nation will be the world’s foremost superpower of the 21st century.

What Is “Quantum” All About?

Quantum theory gives us our best account of nature in the realm of the very small in which particles behave in ways that can seem unnatural. Albert Einstein once colorfully dismissed quantum mechanics as “spooky action at a distance”; however, over the past few decades, physicists have successfully demonstrated the reality of this spooky action.⁶ If quantum physics was adapted into a fictional children’s story—Alice’s Adventures in Quantum Wonderland, perhaps—we could more plainly express what may seem so unnatural or spooky. This fictional children’s story would include quantum principles such as superposition, entanglement, multiplicity, and decoherence.

Superposition describes the fact that quantum particles are in many states *at once* and, interestingly, until the particle is

observed. The state of the particle is best described as a superposition of all those possible states.⁷ If we were reading Alice’s Adventures in Quantum Wonderland, Alice would be everywhere at once—she would be on the riverbank, falling down the rabbit hole, questioning her identity to the blue caterpillar, and arguing with the King and Queen of Hearts all at the same time. However, only when the King and Queen of Hearts observe Alice does she become fixed in a particular state or situation. This version—Alice’s Adventures in Quantum Wonderland—is truly stranger than fiction.

Entanglement is what Einstein was referring to as “spooky action at a distance.” Entanglement links certain quantum particles so that the quantum state of each particle of the group cannot be described independently of the state of the other particle(s), and entanglement can occur over long distances. In the case of Alice’s Adventures in Quantum Wonderland, imagine having the homonym, homophone, homograph, and heteronym words in the book shift states, as these words are “entangled” in the story. Just as the reader can derive the true meaning of the word, physicists can derive the states of entangled quantum particles wherever those words appear in the story. Now that is a spooky action at a distance.

Multiplicity is a phenomenon that allows quantum computers to store a multiplicity of quantum states simultaneously, while classical digital computers can store only one state at a time, or can store many states but in different memory locations. Alice’s Adventures in Quantum Wonderland is a multiple-ending story with many possible outcomes. The reader is never permitted to read all the chapters in one sitting, but over time the reader can document the many different possible endings, resulting in a great appreciation for the complexity of the characters.

Decoherence occurs when quantum bits (qubits) fall out of a state of superposition.⁸ The volatility of qubits can cause data to be lost or altered, which can significantly reduce the accuracy of computational results. The White Rabbit in Alice’s Adventures in Quantum

Wonderland experiences decoherence whenever he attempts to read his pocket watch, at which point the watch stops. In this story the White Rabbit mutters, “Oh dear! Oh dear! I’ve lost the time!” This causes the White Rabbit to “lose” any information regarding the time of day, and he therefore has no appreciation for being late to his duties as herald to the King and Queen of Hearts. In this version of the story, he gladly stops to help Alice after she arrives in Quantum Wonderland and assists her in getting home. This greatly alters the story and makes it highly inaccurate when compared to the original *Alice’s Adventures in Wonderland*.

How Is QC Different?

Most people are familiar with the binary units (1s and 0s) used by classic computer processors. While modern computers use bit processors, QC uses qubit processors with hundreds or even millions of potential combinations, making them ideal for complex computations. The state of qubits does not necessarily reside on either side of the binary spectrum but exists in *both* states through the principle of superposition.⁹ The figure illustrates how superposition introduces immense potential within the field of QC, as the qubits exist in a coherent superposition. A qubit does not have a set value between 0 and 1; rather, qubits have a probability of 0 and a probability of 1. A qubit can be in a combination of *both* states—resulting in enormous processing potential. So how does the processing power of one qubit compare to one bit? It is more a matter of how additional qubits scale. Each additional qubit *doubles* the processing power. For example, three qubits provide 2^3 processing power. Sixty-four qubits provide about 1 million terabytes of processing power—or 18,446,744,073,709,600,000 possibilities.¹⁰

Engineering the qubit today has been compared to the early days of the bit, and ordinary computers, in the 1950s.¹¹ Variations in the design of qubits under development reflect the nascent state of QC. By taking advantage of quantum principles, scientists can use new



Scientists perform calculations on "Taiyuan-1" superconducting quantum computing cloud platform, at Hangzhou International Science and Innovation Center of Zhejiang University, in Hangzhou, Zhejiang Province, July 22, 2022 (Alamy/Cynthia Lee)

algorithms to solve complex problems exponentially faster than even the most advanced super computers in operation.¹²

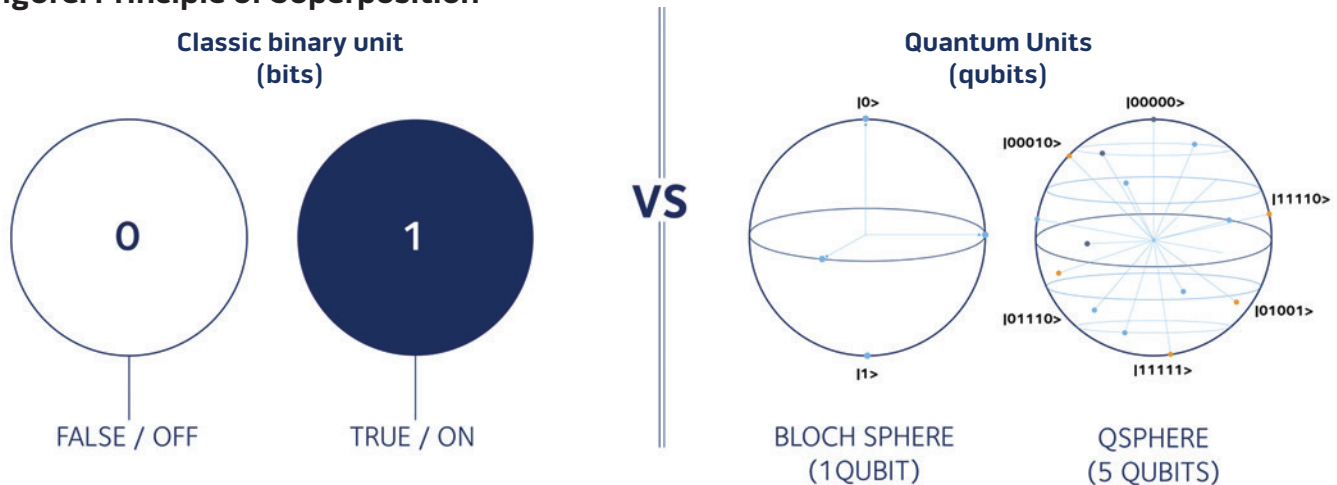
Potential Applications

When discussing applications of quantum technologies, it is critical to note that nearly all existing demonstrations of quantum applications have occurred in highly controlled laboratory

environments and that the success of these tests is not indicative of any near-term potential for commercial or government application. Conceptually, future implementation of quantum mechanics in modern technology will introduce robust real-world applications with significant utility to any agency or commercial entity with the means to procure quantum technologies.

Entire fields are taking shape, aimed at leveraging advancements in technology based off quantum principles. In theory, the strength of quantum technologies is rooted in the timely calculation of complex, large-scale combinatorics problems.¹³ While the list of potential quantum applications is limited compared to the applications of classical computers, quantum applications

Figure. Principle of Superposition



Source: Alexander Fletcher, "Quantum Computing & Financial Technologies," LinkedIn, April 30, 2019.

are growing and evolving as industry continues to uncover computational problem sets that lend themselves to complex combinatorics. Cyber security, advanced materials research, logistics optimization, and weather forecasting all demonstrate promising advancements with Department of Defense (DOD) applications.¹⁴ QC is being developed and tested for applications that will better enable accurate modeling, more complex and simultaneous simulations, more accurate analysis of probabilities, and tackling machine learning and artificial intelligence (AI)-focused problems.¹⁵

Private Sector and Educational Institution Investment

The list of U.S. companies investing in quantum research is extensive. Spending on quantum computers should reach hundreds of millions of dollars in the 2020s and tens of billions in the 2030s.¹⁶ Household names such as Google, Microsoft, and IBM are examples of companies at the forefront of quantum development. Google AI Quantum is currently working to develop open-source tools and novel quantum algorithms that aim

to accelerate machine learning and AI-related tasks.¹⁷ Similarly, Microsoft has established a Quantum Team to address innovations in QC at what they deem “layers of the quantum stack.”¹⁸ This includes providing a collaborative cloud-based environment for quantum developers called Azure Quantum. Microsoft’s Quantum network facilitates partnered quantum development with more than 20 companies and quantum education and research with more than 25 universities. Microsoft also provides a suite of online quantum learning tools to widen the aperture of quantum education. The IBM Quantum Network, made up of more than 100 Fortune 500 companies, universities, and national research laboratories, focuses on accelerated research and development (R&D) of commercial applications and education.¹⁹ These three leaders in industry have taken a similar approach to their investment into quantum R&D. All three promote collaboration with industry and academia, development and distribution of open-source quantum tools, and a fundamental investment into education of the quantum sciences to promote a more capable workforce. U.S. private sector partnerships often cross national

boundaries, and with academic institutions, further complicating what role DOD could or should play.

Quantum Supremacy: China vs. the United States

The term *quantum supremacy* is frequently used as a measure of milestone achievement in quantum technology development. Unlike the military definition, *supremacy* in a QC context refers to a quantum advantage over other systems rather than complete dominance. In October 2019, Google reported reaching quantum supremacy when a quantum computer with a stable 54-qubit processor exceeded the capacity of traditional computers.²⁰ The significance of Google declaring quantum supremacy has been widely debated. Critics claim that loosely structured tasks designed specifically to take advantage of quantum principles were used to declare quantum supremacy and that the task itself was not informative.²¹ Proponents insist that the demonstration illustrates a general understanding of the system, and verification of the output data against the output from traditional systems indicates that the quantum computer is performing as intended. This proof-of-concept demonstration of quantum supremacy is

Table 1. Collaborative Development for Quantum Computing (Representative/Non-Exhaustive)

Companies Developing Quantum Hardware	Academic/Public-Sector Collaborators	Private-Sector Collaborators
IBM	University of Melbourne, Oak Ridge National Laboratory, University of Oxford, Los Alamos National Laboratory, National Taiwan University	JP Morgan, Goldman Sachs, Barclays, ExxonMobil, Samsung, Dupont, Daimler, Mercedes-Benz, Raytheon, Delta Airlines
Google	University of Waterloo, Oak Ridge National Laboratory, NASA, University of California Santa Barbara	Daimler, Volkswagen
Microsoft	Purdue University, Case Western Reserve University, Pacific Northwest National Laboratory, University of Sydney, Technical University of Copenhagen, Eindhoven University of Technology, University of California Santa Barbara, University of Sydney	Honeywell, Dow, Ford, IQBit, Bohr Technology, Cambridge Quantum Computing, Entropica Labs, GTN, OTI Lumionics, ProteinQure, QC Ware, Qulab, QxBranch, Riverlane Research, Solid State AI, Strangeworks, and Zapata Computing
Intel	University of Toronto, University of Chicago, Delft University of Technology	
Biogen		Accenture Labs, IQBit
D-Wave	University of Waterloo, Los Alamos National Laboratory, Oak Ridge National Laboratory	Google, Lockheed Martin, Volkswagen, Amazon Web Services, NEC Corporation
Honeywell		Microsoft, JP Morgan
Rigetti	University of California at Berkeley	Amazon Web Services
Alibaba	University of Science and Technology of China, Chinese Academy of Sciences	

a necessary early step toward developing more useful applications and attracting more investors.

While the incompleteness of open-source information makes it difficult to determine the current winner of the quantum race, a strong case can be made that China is leading the United States in the race for a global QC advantage. In a *Forbes* article titled “Quantum USA vs. Quantum China: The World’s Most Important Technology Race,” Paul Smith-Goodson notes, “One of China’s main goals is to surpass the United States and to become the global high-tech leader. President Xi funded a multi-billion-dollar quantum computing mega-project with the expectation of achieving significant quantum breakthroughs by 2030.”²²

In March 2021, China released its latest five-year strategy, which called for increased investment in advanced technologies such as artificial intelligence and quantum computing. Despite its name, the strategy provides broad goals for China out to 2035, including a 7 percent boost in annual spending on advanced technologies. China hopes this additional R&D investment will create economic independence from the United States as well as bolster its national security. Furthermore, the Congressional Research Service notes, “China is developing strategic technologies and digital infrastructure (including a cryptocurrency) and aims to advance its digital infrastructure and domestic rules globally.”²³ China’s long-term approach to QC is apparent as seven of the top ten universities with QC patents ranked globally are Chinese.²⁴ While quantity does not indicate quality, it is worth noting that Chinese patents from quantum computing outpace the United States 1,657 to 1,439.²⁵

In addition to the threat of China’s own technological advances is the growing threat of the Chinese stealing intellectual property and data. China has increasingly stolen data from DOD and U.S. private industry over the past decade. In 2015, the National Bureau of Asian Research estimated the United States lost \$1.2 trillion in revenue over 3

years as the result of Chinese counterfeiting, piracy, and stolen data.²⁶ Throughout 2018, the Department of Justice indicted Chinese intelligence officials and cyber actors for stealing secrets from U.S. aviation companies as well as intellectual property from other U.S. companies.²⁷

Kari Bingen, former Principal Deputy Under Secretary of Defense for Intelligence, told a subcommittee of the House Armed Services Committee in 2018 that China has made it a priority to maliciously acquire foreign technologies, including those developed within the United States, to advance its economy and to modernize its military.²⁸ In one such example, as late as April 2021, the *Washington Post* reported that FireEye and CISA discovered there was reason to believe that sophisticated Chinese government hackers had infiltrated the information systems of dozens of U.S. Government agencies, defense contractors, financial institutions, and other critical sectors.²⁹ While the extent of the breach is still unknown, FireEye and CISA are already sending out alerts to those affected by the incidents. China’s track record of stealing data from U.S. personnel and companies is clear and persistent, and the security of U.S. information systems will be at significantly greater risk with the fielding of QC technology. These unethical practices of stealing intellectual property give China an advantage over countries that continue to abide by international laws. In the race for quantum supremacy, taking unethical shortcuts may make the difference in who finishes first.

In December 2020, just over a year after Google declared quantum supremacy, a team of researchers from the University of Science and Technology in China declared that *they* had achieved quantum supremacy. The team developed a system called *Jiuzhang*, which manipulated light in the form of photons rather than the super-cold conducting metal used by the Google team. Jiuzhang produced results for its intended task in minutes, compared to the 600 million years it would have taken the world’s most powerful supercomputer to complete.³⁰ The Chinese team, like Google, admitted Jiuzhang was designed only to compute

this specific equation and nothing else.³¹ Even though the scientific community has not verified the authenticity of this experiment and its results, it shows the potential for multiple paths to stabilizing qubits and achieving quantum supremacy.

Most experts assess it will take at least 10 to 20 years before the United States or China builds a mature or fully error-corrected QC capability.³² China is not waiting for the United States to figure out how to build the best quantum computer. Its recent quantum supremacy announcement and increased spending on advanced technology are unsettling when coupled with their track record of stealing data and undermining U.S. interests.

Threats to U.S. Encryption

What would be the risk if China possessed a superior QC capability? DOD top secret networks are protected by a 256-bit Advanced Encryption Standard (AES). To crack this encryption, someone would need to try a maximum of 1.1×10^{77} different key combinations. To put this into perspective, the most powerful computer in 2017 was the Chinese Sunway TaihuLight. This computer, using brute force, would require 885 quadrillion years to crack a 128-bit AES encryption, which is less mathematically complex than the 256-bit AES. The world’s most powerful computer would need more time than the universe has existed to try all number combinations.³³ Taking this into consideration, 256-bit AES is considered the gold standard and quantum resistant. For now, the consensus is that information protected by 256-bit AES is safe; however, unexpected leaps in quantum technological advancements could put the sovereignty of these systems at risk.

Another common type of encryption used by DOD is Rivest-Shamir-Adleman (RSA), which is an encryption method that uses two mathematically linked keys. A public and private key is often used with the DOD Public Key Infrastructure (PKI) and other common unclassified applications. Jon R. Lindsay, in *Strategic Strategies Quarterly*, discusses the mathematical application and security of RSA:

“Modern RSA works because the public key is based on an exceptionally large number (i.e., two to the power of 2048) while the private key is based on its prime factors. . . . A typical desktop computer would need more than six quadrillion years to crack 2048-bit RSA.”³⁴ However, Peter Shor, an American professor of applied mathematics at MIT, may have changed the outlook on the security of RSA. In 1994, Shor developed a quantum algorithm that factors prime numbers for large numbers. Currently, this algorithm is limited by today’s computers and their capabilities. If Shor’s algorithm was coupled with the right capability, such as a quantum computer, then the DOD PKI would be at risk; some experts believe the encryption could be broken in a matter of

hours. Jon A. Lindsay summarized it best when he stated:

*An intelligence adversary with the right kind of machine could potentially break RSA, decrypt classified data, and forge digital signatures. All networks and applications on those networks, public and private, using vulnerable cryptography would be put at risk. Because military operations in all physical environments—land, sea, air, space—rely on many of the same information technologies and networks that power the global economy, a systematic vulnerability in the cyber domain would become a systematic vulnerability in all domains.*³⁵

If China were to successfully create a quantum computer and use it with

Shor’s algorithm, it could create a catastrophic breach for DOD and other government agencies.

U.S. Federal Legislation and Governance

The significance of quantum technology has not been lost on the Federal Government. In 2015, an executive order launched the National Strategic Computing Initiative to advance U.S. leadership in high-performance computing, to include QC.³⁶ In 2018, the U.S. National Science and Technology Council, which coordinates the science and technology policy of the President, developed a National Strategic Overview for Quantum Information Science. Related to this announcement,



Researchers at Air Force Research Laboratory Information Directorate in Rome, New York, advance quantum technologies from individual quantum bit (or qubit) level to system level, January 16, 2015 (U.S. Air Force/Albert Santacroce)



Pleiades supercomputer at NASA Ames is one of many supercomputers used to find limit of quantum supremacy, April 10, 2015 (NASA/Ames Research Center/Dominic Hart)

the National Science Foundation and the Department of Energy (DOE) committed \$249 million to 118 research projects related to quantum information science (QIS).³⁷ In 2019, Executive Order 13885 established the National Quantum Initiative Advisory Committee under the Office of Science and Technology Policy. The committee consists of a director and 22 members appointed by the Secretary of Energy. Committee members represent industry, universities, Federal laboratories, and other Federal agencies.³⁸ The National Quantum Initiative Advisory Committee facilitated the enactment of the National Quantum Initiative Act, which provides an investment mechanism through which the National Science Foundation, National Institute for Standards and Technology (NIST), and DOE can support R&D of quantum technology.³⁹ In response to the National Quantum Initiative Act, the DOE Office of Science launched multiple research programs in QIS with up to \$625 million in funding over 5 years. This includes the standup of five national QIS research centers that focus on diverse collaborative QIS R&D,

technology transfer, and development of the quantum workforce.

While research in many areas of quantum applications is still in its infancy, DOD has been exploring quantum military applications for the past 20 to 30 years.⁴⁰ Recently, the 2020 National Defense Authorization Act (NDAA) allows the secretary of each military Service to “establish or designate a defense laboratory” and mandates that the “Secretary of Defense shall ensure that no less than one such laboratory or center is established or designated.”⁴¹ The Air Force and Navy have since established laboratories dedicated to quantum information sciences and QIS-enabled technologies and systems.⁴² The 2020 NDAA also asks for the Secretary of Defense to submit a report by the end of 2021 to the congressional defense committees on “current and potential threats and risks posed by quantum computing technologies.” The report provides recommendations on how to counter any risks posed by quantum technologies.⁴³ In early 2022, the Office of the Under Secretary of Defense for Research and Engineering released a memo outlining a technology strategy that will “chart a course for the

[U.S.] military to strengthen its technological superiority amidst a global race for technological advantage.” Quantum science is identified as one of 14 critical technology areas vital to maintaining national security.⁴⁴ Congressional leaders are also taking action to ensure that the country’s scientific workforce is prepared to address the emerging quantum threat. In a recent bipartisan effort, legislation proposed in the Senate aims to streamline the DOD and private sector hiring pipeline for students graduating with degrees related to the quantum sciences.⁴⁵ If passed, this legislation would signify a large U.S. investment in its future quantum intellectual capital.

Other key quantum technology stakeholders within the Federal Government include the National Aeronautics and Space Administration (NASA) and the Department of Commerce. NASA’s Quantum Artificial Intelligence Laboratory collaborates with multiple hardware development and research groups such as Google to conduct tests on near-quantum computing hardware, with the goal of evaluating the potential of quantum computing capabilities.⁴⁶ The Department of Commerce, through

NIST, is also deeply invested in quantum research. NIST conducts quantum-based research through partnerships with academic institutions. One such effort is the Joint Quantum Institute, a collaborative research endeavor among the University of Maryland, NIST, and the Laboratory for Physical Sciences, which conducts research in the fields of quantum computing, quantum many-body physics, and quantum control, measurement, and sensing.⁴⁷

President John F. Kennedy's national priority of beating the Soviets to the moon may be comparable to the current race against China to harness the potential of the quantum, though not nearly as well recognized by the public. Each milestone reinforces global dominance and undoubtedly unlocks potentially disruptive technologies to national and global economies. The U.S. Government requested \$844 million for quantum information science R&D in fiscal year (FY) 2023, which is an 8 percent decrease from FY2022.⁴⁸ When compared to the space race in the 1960s, the United States similarly spent \$903 million on the Apollo and related programs in 1960 (adjusted for inflation in FY2020).⁴⁹ Spending on the Apollo and related programs then peaked in 1965 at \$40.9 billion—48 times greater.

Recommendations

Since 1989, U.S. military strategy has been defined in terms of ends, ways, and means, which provides a framework for military strategy and offers a lens for subsequent types of planning.⁵⁰ This same approach can be used to establish a simple yet effective strategic framework for quantum technology development and integration into DOD systems.

The end (that is, what the objective is) for DOD when it comes to QC is mitigating the potential threats to the homeland enabled by quantum technological advancements. Since China is already invested heavily in quantum technologies with a long-term outlook, DOD should assume that QC poses a long-term threat to homeland defense. The end includes a mature, secure, and profitable QC industry that benefits society in various ways that justify the investment.

The way (how the objective will be achieved) is an engaged and informed DOD and Federal Government that will mitigate the threat and better enable the United States and its allies to achieve a quantum advantage over its adversaries. The United States and its allies must develop a reliable and robust QC capability and the knowledge of how to harness that capability before the Chinese establish a true quantum advantage. DOD must efficiently and effectively integrate with industry and academia into a whole-of-society approach to quantum innovation that promotes intellectual synergy, while simultaneously ensuring that these efforts align with national security interests. DOD should continue to actively pursue collaboration with other government agencies, the private sector, academic institutions, and its allies and constituents abroad. These partnerships will enable DOD to advocate for government collaboration on projects with an increased focus on protecting advances in quantum R&D from habitual thieves of U.S. intellectual property. These partnerships will allow DOD to shepherd targeted research toward areas advantageous to national security and homeland defense while allowing companies in the private sector autonomy on projects not directly tied to DOD. Moreover, the ways can be achieved via well-informed organizations with common goals that underlie national defense.

DOD also needs to examine challenges within its own acquisition processes to remain ahead of the pacing quantum threat.⁵¹ In January 2020, DOD established the Adaptive Acquisition Framework in DOD Instruction (DODI) 5000.02, which affords program managers the flexibility to tailor an acquisition between six different acquisition pathways.⁵² Tailoring pathways for specific requirements is intended to better allow for more timely and less costly acquisitions. While such policy changes are laudable, DOD should provide specific guidance regarding the acquisition of quantum-based technologies in a future iteration of DODI 5000.82, *Acquisition of Information Technology*, as quantum-based technologies will present

unique challenges to the acquisition process and will likely prove disruptive to established technologies.

Federal Government programs that support technological innovations and expedite critical acquisitions may not sufficiently target DOD challenges with quantum-based technologies. The Small Business Innovation Research and Small Business Technology Transfer programs are targeted at innovation but are limited to small businesses and have contract thresholds that likely exclude many of the large businesses that are already heavily invested in QC R&D. Sole-source contracts are intended to reduce the acquisition timeline by excluding competition in certain circumstances. Per the Federal Acquisition Regulation, a sole-source contract may be awarded if the supply or service “demonstrates a unique and innovative concept or demonstrates a unique capability of the source to provide the particular research services proposed.”⁵³ However, there is no obligation for the company to enter a contract with DOD. Furthermore, any company would have an incredible amount of negotiating leverage over DOD as that technology becomes more viable and potentially a threat to homeland defense. Awarding contracts in a timely manner and efficiently (when most needed) to compel advancements in quantum computing will be essential for the Federal Government and DOD.

The primary means (the resources necessary to implement the strategy) for DOD is earmarked funding and, to a lesser degree, dedicated manpower. DOD must have sufficient funding to advance QC. Targeted funding for R&D could result in effects that are advantageous to U.S. national security and the national economy. U.S. spending on QC should be benchmarked as a percentage of gross domestic product and tied to spending by the Chinese at a minimum. The threat to homeland defense also necessitates dedicated DOD manning for addressing QC challenges now. While a whole-of-society approach has begun for DOD, QC will eventually necessitate a restructuring of command and control. The National Security Agency and its

partners U.S. Cyber Command, U.S. Northern Command, and CISA are best equipped to address QC risks based on their information mission sets. Quantum research in the field of cyber security is a particular area of interest and investment for DOD. While DOD is heavily invested in its broadly defined role within the larger National Quantum Initiative, dedicating money and intellectual capital to an R&D effort that focuses on cyber security challenges of quantum within the realm of DOD cyber infrastructure is paramount to the maintained sovereignty of critical information systems.

Conclusion

Some of America's brightest minds are actively researching the vast potential of quantum computing. DOD is likely going to play an essential role within the field of QC, and projected spending indicates that role will increase going forward. The DOD role in developing state-of-the-art technologies ensures that the commercialization of QC will be heavily influenced by the agency. Unlike its counterparts in the private sector and academia, DOD has a defined obligation for defense of the homeland, as stated in the National Security Strategy and National Defense Strategy.

Falling behind other nations will significantly increase security risks to the United States, not the least of which is the compromise of U.S. public or private information systems via malign cyber attacks. This threat necessitates that DOD increase its role in emerging QC technologies, including those related to quantum cryptography and nonquantum technologies considered quantum resistant. In a worst-case scenario, China prioritizes quantum technology R&D more than the United States, continues to invest heavily, and achieves a quantum advantage independently, leaving the United States behind.

While the consensus within the scientific community is that mature (or fully error-corrected) quantum computers are a decade or more from realistically becoming a threat to the United States, DOD must actively remain engaged to accurately assess risks. The U.S.

Government, private sector, national laboratories, and academic institutions have already invested significant time and funding to address the quantum challenge in a collaborative environment; however, DOD's role must be better aligned with the strategic risks to homeland defense. Failure by DOD to fully understand the strategic landscape or to delay seizing the initiative within the field of quantum computing will result in a disadvantage that the United States cannot afford. JFQ

Notes

¹ Aaron Gregg, Sean Sullivan, and Stephanie Hunt, "As Colonial Pipeline Recovers from Cyberattack, Leaders Point to a 'Wake-Up Call' for U.S. Energy Infrastructure," *Washington Post*, May 13, 2021, <https://www.washingtonpost.com/business/2021/05/13/colonial-pipeline-ransomware-gas-shortages/>.

² Will Englund and Ellen Nakashima, "Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operations," *Washington Post*, May 12, 2021, <https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/>.

³ "Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware," Cybersecurity & Infrastructure Security Agency, May 11, 2021, <https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware>.

⁴ Dorothy E. Denning, "Is Quantum Computing a Cybersecurity Threat?" *American Scientist* 107, no. 2 (March–April 2019), 83–85, <https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat>.

⁵ Ibid.

⁶ Gabriel Popkin, "Einstein's 'Spooky Action at a Distance' Spotted in Objects Almost Big Enough to See," *Science*, April 25, 2018, <https://www.sciencemag.org/news/2018/04/einstein-s-spooky-action-distance-spotted-objects-almost-big-enough-see>.

⁷ Scott Buchholz et al., "The Realist's Guide to Quantum Technology and National Security," *Deloitte Insights*, February 6, 2020, <https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html>.

⁸ Philip Ball, "The Universe Is Always Looking," *The Atlantic*, October 20, 2018, <https://www.theatlantic.com/science/archive/2018/10/beyond-weird-decoherence-quantum-weirdness-schrodingers-cat/573448/>.

⁹ *Quantiki* (October 26, 2015), s.v. "qubit," <https://www.quantiki.org/wiki/qubit>.

¹⁰ Cathal O'Connell, "Quantum Computing for the Qubit Curious," *Cosmos*, July 5, 2019,

<https://cosmosmagazine.com/physics/quantum-computing-for-the-qubit-curious/>.

¹¹ Adrian Cho, "No Room for Error," *Science*, July 9, 2020, <https://www.sciencemag.org/news/2020/07/biggest-flipping-challenge-quantum-computing>.

¹² Max G. Levy, "New Quantum Algorithms Finally Crack Nonlinear Equations," *Quanta Magazine*, January 5, 2021, <https://www.quantamagazine.org/new-quantum-algorithms-finally-crack-nonlinear-equations-20210105/>.

¹³ Francesco Bova, Avi Goldfarb, and Roger G. Melko, "Commercial Applications of Quantum Computing," *EPJ Quantum Technology* 8, no. 2 (January 2021), <https://doi.org/10.1140/epjqt/s40507-021-00091-1>.

¹⁴ Stephen Gossett, "10 Quantum Computing Applications and Examples," *Built In*, June 8, 2022, <https://builtin.com/hardware/quantum-computing-applications>; Scott Buchholz, Caroline Brown, and Deborah Golden, "A Business Leader's Guide to Quantum Technology," *Deloitte Insights*, April 15, 2021, <https://www2.deloitte.com/us/en/insights/topics/innovation/quantum-computing-business-applications.html>.

¹⁵ Gossett, "10 Quantum Computing Applications and Examples."

¹⁶ Duncan Stuart, "Quantum Computers: The Next Supercomputers, but Not the Next Laptops," *Deloitte Insights*, December 11, 2019, <https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/quantum-computing-supremacy.html>.

¹⁷ "Explore the Possibilities of Quantum," Google Quantum AI, n.d., <https://research.google/teams/applied-science/quantum/>.

¹⁸ "Azure Quantum," Microsoft Azure, 2023, <https://azure.microsoft.com/en-us/solutions/quantum-computing/>.

¹⁹ IBM Quantum, IBM, n.d., <https://www.ibm.com/quantum-computing/>.

²⁰ Frank Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature*, October 23, 2019, <https://www.nature.com/articles/s41586-019-1666-5>.

²¹ John Preskill, "Why I Called It 'Quantum Supremacy,'" *Quanta Magazine*, October 2, 2019, <https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/>.

²² Paul Smith-Goodson, "Quantum USA vs. Quantum China: The World's Most Important Technology Race," *Forbes*, October 10, 2019, <https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=46c1c62272de>.

²³ "China's 14th Five-Year Plan: A First Look," *Congressional Research Service*, January 5, 2021, <https://crsreports.congress.gov/product/pdf/IF/IF11684>.

²⁴ "Infographics on Quantum Computing: Patent Trends and Analysis," PatSeer, n.d.,

<https://patseer.com/infographics-on-quantum-computing-patent-trends-and-analysis/>.
²⁵ Ibid.

²⁶ *The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, update to the *Intellectual Property Commission Report* (Washington, DC: National Bureau of Asian Research, 2017), <https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/>.

²⁷ “Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies,” Department of Justice, October 10, 2018, <https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading>; “Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information,” Department of Justice, December 20, 2018, <https://www.justice.gov/usao-sdny/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer>.

²⁸ Lisa Ferdinando, “DOD Officials: Chinese Actions Threaten U.S. Technological, Industrial Base,” Department of Defense, June 21, 2018, <https://www.defense.gov/News/News-Stories/Article/Article/1557188/dod-officials-chinese-actions-threaten-us-technological-industrial-base/>.

²⁹ Ellen Nakashima and Aaron Schaffer, “Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors,” *Washington Post*, April 21, 2021, https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html.

³⁰ Becky Bracken, “Chinese Breakthrough in Quantum Computing a Warning for Security Teams,” *Threatpost*, December 7, 2020, <https://threatpost.com/chinese-quantum-computing-warning-security/161935/>; Zen Chan, “A Leap of Quantum Computing in China, a Threat to Internet Security,” *01*, February 2, 2021, <https://vocal.media/01/a-leap-of-quantum-computing-in-china-a-threat-to-internet-security>; Tom Simonite, “China Stakes Its Claim to Quantum Supremacy,” *Wired*, December 3, 2020, <https://www.wired.com/story/china-stakes-claim-quantum-supremacy/>.

³¹ Emily Conover, “The New Light-Based Quantum Computer Jiuzhang Has Achieved Quantum Supremacy,” *Science News*, December 3, 2020, <https://www.sciencenews.org/article/new-light-based-quantum-computer-jiuzhang-supremacy>.

³² Lamont Wood, “The Clock Is Ticking for Encryption,” *Computerworld*, March 21, 2011, <https://www.computerworld.com/article/2550008/the-clock-is-ticking-for-encryption.html#:~:text=But%20using%20quantum%20technology%20with>.

³³ Douglas Crawford, “How Does AES

Encryption Work?” *ProPrivacy*, February 4, 2019, <https://proprivacy.com/guides/aes-encryption>; Benjamin Scott, “Military-Grade Encryption Explained,” *NordPass*, August 12, 2020, <https://nordpass.com/blog/military-grade-encryption-explained/#:~:text=Military%2Dgrade%20encryption%20refers%20to>.

³⁴ John R. Lindsay, “Surviving the Quantum Cryptocalypse,” *Strategic Studies Quarterly* 14, no. 2 (Summer 2020), 49–73.

³⁵ Ibid.

³⁶ Executive Order 13702, *Creating a National Strategic Computing Initiative* (Washington, DC: The White House, July 29, 2015), <https://irp.fas.org/offdocs/eo/eo-13702.pdf>.

³⁷ Hamish Johnston, “U.S. Invests \$249m in Quantum Information Science as White House Unveils Strategic Overview,” *Physics World*, September 28, 2018, <https://physicsworld.com/a/us-invests-249m-in-quantum-information-science-as-white-house-unveils-strategic-overview/>.

³⁸ Executive Order 13885, *Establishing the National Quantum Initiative Advisory Committee* (Washington, DC: The White House, August 30, 2019), <https://www.govinfo.gov/content/pkg/DCPD-201900584/pdf/DCPD-201900584.pdf>.

³⁹ Akhil Iyer, *Tech Factsheets for Policymakers: Quantum Computing* (Cambridge, MA: Belfer Center for Science and International Affairs, 2020), https://www.belfercenter.org/sites/default/files/files/publication/QC_2.pdf.

⁴⁰ David Vergun, “DOD Officials Discuss Quantum Science, 5G and Directed Energy,” *DOD*, March 9, 2021, <https://www.defense.gov/Explore/News/Article/Article/2530494/dod-officials-discuss-quantum-science-5g-and-directed-energy/>.

⁴¹ *National Defense Authorization Act for Fiscal Year 2020*, S. 1790, 116th Cong., 1st sess., January 3, 2019, <https://www.congress.gov/116/bills/s/1790/BILLS-116s1790enr.pdf>.

⁴² Brandi Vincent, “Inside the Air Force Research Laboratory’s Contemporary Quantum Pursuits,” *Nextgov*, January 6, 2021, <https://www.nextgov.com/emerging-tech/2021/01/inside-air-force-research-laboratory-contemporary-quantum-pursuits/171201/>; Paul Cage, “Naval Research Laboratory Designated Navy’s Quantum Information Research Center,” U.S. Navy Office of Information, September 28, 2020, <https://www.navy.mil/Press-Office/News-Stories/Article/2364183/naval-research-laboratory-designated-navys-quantum-information-research-center/>.

⁴³ Dwight Weingarten, “House Panel Approves NDAA Cyber, Quantum Provisions,” *MeriTalk*, June 22, 2020, <https://www.meritalk.com/articles/house-panel-proves-ndaa-cyber-quantum-provisions/>.

⁴⁴ “USD(R&E) Technology Vision for an Era of Competition,” Under Secretary of Defense for Research and Engineering, February 1, 2022, [https://www.cto.mil/wp-content/](https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf)

[uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf](https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf).

⁴⁵ William McCormick, “Senators Introduce Legislation to Assist DOD Quantum Computing Efforts; Sen. Maggie Hassan Quote,” *ExecutiveGov*, April 16, 2021, <https://www.executivegov.com/2021/04/senators-introduce-legislation-to-assist-dod-quantum-computing-efforts-sen-maggie-hassan-quote/>.

⁴⁶ “NASA Quantum Artificial Intelligence Laboratory (QuAIL),” National Aeronautics and Space Administration, November 9, 2022, <https://www.nasa.gov/content/nasa-quantum-artificial-intelligence-laboratory-quail>.

⁴⁷ “Research,” Joint Quantum Institute, n.d., <https://jq.i.umd.edu/research>.

⁴⁸ *National Quantum Initiative Supplement to the President’s FY 2023 Budget: A Report by the Subcommittee on Quantum Information Science, Committee on Science of the National Science & Technology Council (NSTC)* (Washington, DC: NSTC, January 2023), <https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf>.

⁴⁹ “Project Apollo Cost Data: Project Apollo 1960–1973,” comp. Casey Drier, The Planetary Society, https://docs.google.com/spreadsheets/d/e/2PACX-1vTKMekJW9F8Z3f-Wnx-IxvHSPD35iZxZxVVoqIp25FxxXjO-qJ2Rk-zS858dNDON_3cwacblX8gr9xt/pubhtml.

⁵⁰ Ian King, “Beyond Ends, Ways, and Means: We Need a Better Strategic Framework to Win in an Era of Great Power Competition,” *Modern War Institute*, September 3, 2020, <https://mwi.usma.edu/beyond-ends-ways-and-means-we-need-a-better-strategic-framework-to-win-in-an-era-of-great-power-competition/>.

⁵¹ A 2017 Government Accountability Office (GAO) report identified six areas that innovative companies had cited as challenges that deter them from working with DOD: complexity of DOD’s process, unstable budget environment, long contracting timelines, intellectual property rights concerns, government-specific contract terms and conditions, and an inexperienced DOD contracting workforce. See “Military Acquisitions: DOD Is Taking Steps to Address Challenges Faced by Certain Companies,” GAO-17-644 (Washington, DC: GAO, July 20, 2017), <https://www.gao.gov/products/gao-17-644>.

⁵² DOD Instruction 5000.02, *Operation of the Adaptive Acquisition Framework* (Washington, DC: DOD, January 23, 2020, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.PDF>).

⁵³ Federal Acquisition Regulation, Part 6.302, “Circumstances Permitting Other Than Full and Open Competition,” *Acquisition.gov*, December 30, 2022, https://www.acquisition.gov/far/part-6#FAR_6_302.



Soldiers check Nett Warrior end-user devices during Army Expeditionary Warrior Experiment force-on-force field demonstration held on Fort Moore (formerly Fort Benning), Georgia, March 4, 2021 (U.S. Army/Jason Amadi)

An AI-Ready Military Workforce

By Iain Cruickshank

Much recent professional military writing, such as the National Security Commission on Artificial Intelligence's *Final Report*, stresses the need for an artificial intelligence (AI)-ready workforce.¹ AI has the distinct potential for creating a battlefield advantage for whichever warring party can best harness the

technology, making an AI-ready military workforce imperative to gaining that advantage.² Thus, while it is generally clear that the military needs an AI-ready workforce, what that should actually mean is less clear.

Most commentators in this area vaguely suggest “AI experts in uniform” as the solution to an AI-ready workforce for the military.³ Recent work has indicated that there are distinct roles in the production of AI as well as distinctive training needs for different

roles.⁴ Additionally, commentators have pointed out the need for some level of understanding of AI for senior leaders, acquisitions personnel, and users of AI-enabled systems.⁵ Despite the recent scholarship identifying different relationships to AI within the workforce, there is no unifying model of an AI-ready workforce that considers such needs as the scale of the different parts of the workforce. AI workforce proposals to date only consider creating an AI-enabled system (for instance, running

Dr. Iain Cruickshank is a Senior Researcher at the United States Military Academy at West Point.

an AI project, creating a model from scratch) or running a full data science project. Moreover, they ignore more realistic uses of AI in military settings, which include tasks such as maintaining and adjusting models to changes in the operational environment.

In this article, I argue that an AI-ready workforce for the military should be built around an AI skills-in-depth model that:

- creates gradations of AI technical skills that address the actual demands AI-enabled technologies will place on a military force
- focuses on educating leadership and the acquisitions community on recognizing opportunities to use AI and evaluating AI capabilities
- prioritizes creation of lower skilled technicians in uniform over creating higher skilled AI experts in uniform.

Before exploring the proposed model for what an AI-ready workforce looks like for a military Service, it is important to clarify a few points about the use of AI. First, AI-enabled systems require maintenance. Machine learning algorithms, which are at the heart of an AI-enabled system, suffer from many issues, including model drift, changes in the data generation environment, issues with models being deployed in real life, and newer, better models coming out.⁶ These

inherent issues with AI-enabled systems mean that they will require periodic maintenance, updating, and monitoring for changes in model performance or data input to continue to be useful. Second, the application of AI requires careful consideration of the problem. AI is not a catch-all that can solve any problem. AI-enabled systems typically need to be tailored to a specific problem, which requires thought about what problems are amenable to AI solutions and how to implement those solutions in a way that works for the organization.⁷ Third, AI will often come as part of a larger integrated system. The actual machine learning that makes up any AI-enabled system is typically one relatively small component, which is commonly just one component of a larger system, like the autonomous threat recognition algorithm for a mobile autonomous platform.⁸ When using an AI-enabled system for a real-world problem, it is important to remember that that system will require maintenance and that machine learning models will only be narrowly applicable to a given problem.

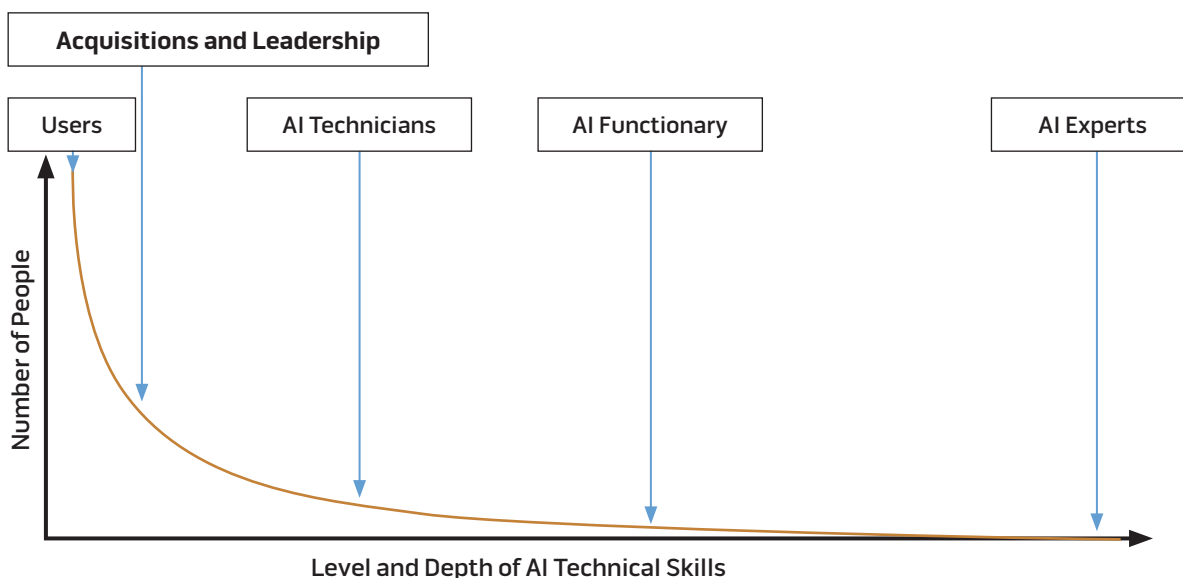
From these fundamental observations, we can deduce the rough outlines of what AI will look like in the military, even if particular details are missing. AI will be present in many, if not most, battlefield systems, from vehicles to mission command suites, and built in as core

components of those battlefield systems by defense contractors. All of these AI-enabled systems and their associated machine learning models will require maintenance, at least some of which will need to be conducted by uniformed personnel. There will also likely be a need for ad hoc data science and AI solutions created within military units to support a particular commander or battlefield problem. Thus, interactions with AI-enabled systems will be predominantly confined to the user level, followed by much fewer maintenance types of interactions, and very few design-and-implement kinds of interactions.

Outline of an AI-Enabled Military Workforce

Given the real-world demands of using AI in the military, the best way to create an AI-ready workforce is to follow an AI skills-in-depth model of training and education. This model must economize resources while also producing a military workforce that can actually harness the battlefield advantages offered by AI. While no part of the model is sufficient to create an AI-enabled workforce, each part addresses a necessary component, and when combined they are sufficient to achieve the desired endstate. The model's fundamental dynamic can be summarized as exponentially decreasing the numbers of military workforce

Figure 1. AI Skills-in-Depth Model



members in work roles as we increase the AI technical skills required for those work roles. This decrease is done for two primary reasons. First, as the level of expertise in AI technical skills increases, the “cost” to create proficiency with those skills increases exponentially. Second, this model will decrease the number of Servicemember interactions with the AI-enabled systems that require specialist AI technical skills. Figure 1 summarizes the model and its different components. Each of the components (that is, users, AI technicians, and so forth) is described in detail in the table.

Another way of thinking about the AI skills-in-depth model is by the relative amount of time members of each of the components spend on hands-on work using AI skills. For example, at the user level, the hands-on AI technical work will largely consist of being aware

of when the AI-enabled system is not working properly. This means that little of their working time will be spent on hands-on AI-technical work, whereas an AI technician or functionary, who will have to perform hands-on AI technical tasks (such as fine-tuning models, checking a model’s performance against new data, checking data integrity), will need significantly more time to perform those tasks (perhaps equating a second job or additional duty). Figure 2 displays the dynamic of the amount of working time needed to perform AI technical skills as part of the job.

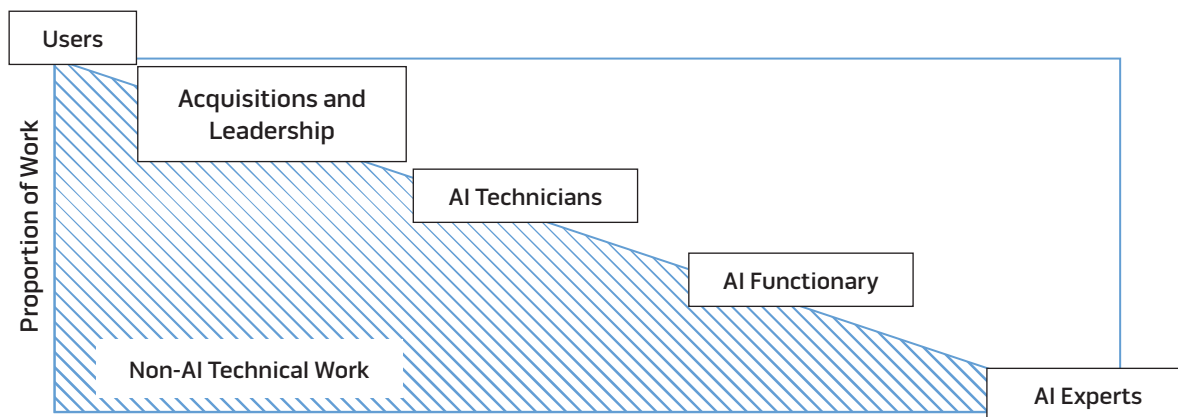
This model closely resembles what is already in place in various military communities. One example is the military medical community; the U.S. Army trains all of its personnel on emergency medical procedures. This type of training is roughly analogous to what is needed within the AI users’ component. On the

battlefield, the Army has medics at the unit level providing limited emergency (tactical casualty care) medical care. The next level is the aid station, possibly staffed with a physician assistant and registered nurse, both of whom possess greater medical expertise and require more medical education and training. They are capable of the next level of medical care and getting the patient stabilized. These individuals and their respective levels of skills are roughly analogous to the AI technicians and functionaries when it comes to working on an AI-enabled system. Eventually, the casualty may get transported to a full trauma center to receive lifesaving surgery, which is performed by surgeons, who require more medical education and training than the previous layers. These individuals are roughly analogous to those individuals in the AI experts component. A layered approach to functional expertise is already

Table. Summary of the Different Layers of the Expertise-in-Depth Model for an AI-Ready Military Workforce

Component	Part of Workforce	Skills Requirement	Time Requirement	Description
User	Vast majority of the workforce	How to employ relevant AI-enabled technologies with a very brief high-level knowledge of AI	A few hours to a day or two, augmented with on-the-job experience	Training meant to make members of the workforce comfortable and effective with using relevant AI-enabled technologies and understanding general capabilities and limits
Acquisitions and Leadership	Mid-to-senior leadership levels along with the acquisitions workforce	Knowledge of AI concepts and high-level workings and requirements of AI-enabled systems. Knowledge of trends and likely near-term future AI technologies.	A couple of weeks to a couple of months	Short education course meant to help leaders and the acquisition workforce identify problems suitable for AI solutions and evaluate proposed solutions. Initial education followed by periodic refresher training.
AI Technician	Select individuals that have a responsibility to maintain one or more AI-enabled systems	Expertise in elements of maintaining an AI-enabled system, including model fine-tuning, model monitoring, and data monitoring	Several months to a year	Education course with supervised hands-on experience maintaining various aspects of an AI-enabled system
AI Functionary	Select individuals that have a need to create novel AI solutions and develop limited scope systems	Expertise in usage of AI-enabled systems to include designing and implementing basic AI solutions, performing exploratory data analysis, creating machine learning pipelines	2 to 4 years	Extended education course (for example, formal academic education) that teaches both some theory of AI and application of AI to problems along with supervised hands-on experience
AI Expert	Specialty personnel whose job it is to build, design, and research AI-enabled systems for the military	Expertise in the design, theory, and usage of AI-enabled systems	5+ years	Extended education courses (for example, formal academic education) that covers everything from theory through implementation of AI. Research experience in an AI field and lots of practical experience with creating state-of-the-art AI and implementing AI solutions.

Figure 2. Relative Amount of Time Spent Performing AI-Technical Tasks



extant in some military functions, like military medicine.

More concretely, the model consists of five different components—users, leaders and acquisitions experts, technicians, functionaries, and experts—of AI training and education that differ in their hands-on AI technical skills and scope of interaction with military AI-enabled systems. These components, when combined, allow for a robust and realizable AI-ready workforce that can meet all the demands that incorporating AI into warfighting will place on the workforce. The table summarizes the different components of the AI skills-in-depth model.

Given the predicted profusion of AI-enabled systems and equipment on the battlefield, it is likely that most military members will have to interact with AI-enabled technology, and most interactions with AI-enabled technologies will occur at the user level.⁹ Thus, it is necessary to train the workforce on how to properly use their AI-enabled technologies so that users trust their equipment and can effectively and ethically use it. To achieve these effects, this training should naturally include some instruction in the high-level concepts of the technology powering the system, like machine learning. Training will also need to include the skills to detect/identify when the technology is not functioning properly. However, malfunctioning AI-enabled technologies will be, to a great degree, application-specific (that is, Google Maps malfunctions for different reasons than a detection model in a digital camera).

Something like new equipment training, which is part of the standard fielding process for the Army, would be a good place to incorporate this type of user-level training.¹⁰ Other forces outside of the United States have also similarly recommended and outlined training for users of AI-enabled systems.¹¹ Generally, the proposed training of this layer only requires basic knowledge of AI. Users practice within their respective fields; the practice of that field could be improved by using AI-enabled technologies but does not require any hands-on technical work in AI.

The next component in the model consists of the military leaders and the acquisitions experts of the workforce. This education is meant to bring leaders a big-picture understanding of AI function and some of its technological applications to best identify problems that are amenable to AI solutions. To successfully utilize AI-enabled technologies in military operations, just like any other combat enabler, a military leader must possess sufficient knowledge of the enabler. Introducing education on AI into intermediate and senior Service college curriculums would accomplish this. The Army's Military Intelligence Center of Excellence is already pioneering training of this type for their warrant officer advanced course wherein students are given a high-level overview of machine learning, what it looks like when AI-enabled systems go wrong, and the military intelligence functions in which students may come across these AI-enabled technologies.¹² The course instructors also challenge students

to identify a problem in their own workflows that could be addressed by an AI-enabled solution and how they could plan to implement that solution. Within the joint community, the chief digital and artificial intelligence office is currently experimenting with a "Lead AI" course that pursues similar goals and strives to create awareness of AI capabilities for senior leaders.¹³ Training leaders so that they know what AI can provide and challenging them to think about what functions or roles they perform that could benefit from AI will greatly speed the creation of an AI-ready military.

Additionally, since the design and production of AI-enabled technologies continue to be the domain of defense contractors, it is important for personnel involved in the acquisitions process to possess appreciable AI knowledge. Since civilian AI experts will not necessarily understand the military problems that they will build AI solutions for, and military personnel may not necessarily understand the AI technology, these personnel need to bridge that gap. It is vital to the health of the force that acquisitions personnel be able to evaluate proposed solutions and ensure AI is properly incorporated into military systems. Other commentators have remarked on this need for AI training for acquisitions personnel,¹⁴ and there has been some recent work outlining AI-specific checks for military projects in the development phase.¹⁵ While this layer of the AI-enabled workforce could benefit from some practice and expertise in AI, neither of these two workforce functions



Joint Department of Defense team executed 12 artificial intelligence flight tests in which AI agents piloted X-62A Variable Stability In-Flight Simulator Test Aircraft, seen here in an August 26, 2022, photo, to perform advanced fighter maneuvers at Edwards Air Force Base, California, December 1–16, 2022 (U.S. Air Force/Kyle Brasier)

requires that these personnel be AI practitioners to carry out their respective organizational functions.

It should also be noted that there is considerable complexity in terms of processes and roles within the military's acquisition workforce and that the need for AI technical expertise will likely vary significantly across the acquisitions enterprise. For example, individuals involved in testing and evaluating a possible new system will likely require more AI technical skills than those involved in project management or contracting. The acquisitions component in this model is meant to apply to the more major and generic functions of acquisitions.

The AI technicians component is comprised of individuals who are primarily responsible for maintaining

AI-enabled systems, which will require maintenance of their machine learning models and data pipelines. This maintenance will require some hands-on (but not expert level) AI technical skills. Students will require hands-on experience with machine learning-related skills, like model fine-tuning, and running AI enablers, like cloud instances. The Army's Artificial Intelligence Integration Center is set to begin the third iteration of its AI Cloud technician's course, which serves as a good starting place for this technician-level of training and education.¹⁶ Students in the course are taught Python programming, along with cloud administration and some basic skills in modification of machine learning models. Following the classroom instruction, students have a utilization tour wherein,

ideally, they can further hone their skills. While this program is a good start, these technician programs will likely need to be expanded and focused around certain maintenance functions of AI-enabled systems in the future, to include machine learning model maintenance and data curation. The chief digital and artificial intelligence office has also highlighted a worker archetype, "Embed AI," which would cover this role as well (although it does not appear to have any training associated with the role).¹⁷ At the technician's layer, the workforce will need education that includes hands-on practice with the maintenance aspects of AI.

Closely related to AI technicians are AI functionaries. The maintenance of AI-enabled systems will occasionally require more detailed skills in larger, more



complex machine learning operations at higher echelons.¹⁸ There will also be the need for ad hoc and customized data science and AI solutions to specific unit and battlefield problems. Some units, such as the 513th Military Intelligence Brigade, have already experimented with this concept by having a unit data scientist officer who can deliver quick simple machine learning solutions to unit problems.¹⁹ At this layer, students will need not only a greater depth of hands-on technical skills than at the previous layer but also a greater breadth of knowledge across more elements of an AI-enabled system. This type of work will likely require experiential learning that can only be imparted at this time by a higher level education program. As an example, the Army's Artificial Intelligence Integration

Center is running its second iteration of the AI scholars' program.²⁰ Army company-grade officers are sent to graduate school to obtain a master's degree in an AI-relevant field, followed by a utilization tour with the Artificial Intelligence Integration Center to, ideally, further refine and practice their skills. The U.S. Air Force produces similar results with its Air Force Accelerator program.²¹ At this layer, the workforce will need both more breadth and depth of practiced skills in AI; however, there will likely be relatively few interactions that will need this level of skills within a military organization.

Then, there are the experts in AI: the professionals who are dedicated to practicing AI, with a high level of education and practical experience in their relevant AI fields. Their profession is

exclusively doing AI. They are also very expensive to produce, not only from the educational perspective, because they often require top-level degrees, but also from the investment of time in their practice. Furthermore, to really be able to grow, retain, and employ these individuals, even at a basic level, the military would have to *significantly* change its manning practices, as has been outlined in the National Security Commission on Artificial Intelligence's *Final Report* and argued by other authors.²² Because there are relatively few interactions with AI-enabled military systems that require a true expert, experts can fall out of practice with critical skills. This is costly both because of the initial investment in such specialized skills and then the loss of those skills from disuse. Thus, while



U.S. Central Command Chief Technology Officer Schuyler Moore (left) and Army Sergeant Mickey Reeves, winner of U.S. Central Command's 2022 Innovation Oasis, conduct press briefing on artificial intelligence and unmanned systems at Pentagon, Washington, DC, December 7, 2022 (DOD/Alexander Kubitzka)

experts are absolutely needed, the force should prioritize using fewer experts more effectively until the demands of AI-enabled warfare grow and battlefield experience can clarify where investments in expertise are needed.

It is important for military decision-makers not to become fixated on having the best-of-the-best AI practitioners at the expense of having broad exposure to AI skills in uniform. Finally, it is also worth pointing out, as other commentators have,²³ that a method of service like Component 3 (Army Reserve) units might be more conducive to growing AI experts for the military workforce than other modes of service, like Component 1 (Active Duty). The 75th Innovation Command is a Component 3 unit assigned to the Army Futures Command that would be a good place to grow AI experts. Most Component 3 personnel

also have a civilian career, and some might already work in science, technology, engineering, and mathematics fields to include AI/machine learning. Reserve Component service, combined with enablers like remote work, presents the ability for AI experts to largely stay practitioners in their fields, but the military establishment still has the ability to leverage them when an AI expert is actually needed.

Finally, while there is a certain hierarchy present in the model in terms of the number of people and time spent doing hands-on technical work in the model, the skills needed for each component do not necessarily overlap. For example, a skill such as fine-tuning a pretrained model will be shared by AI technicians and all the components above that component (AI functionary, AI expert), but other skills, like strategic planning for AI

employment or project management, do not translate up the hierarchy. The hierarchy present in the model also does not necessarily imply level of expertise as well. For example, an AI technician could be an expert at fine-tuning computer vision models, while an AI expert in something like reinforcement learning models may have only a basic level of expertise. While expertise and skills generally increase as one moves up the hierarchy in the model, this is not always the case.

Closing Thoughts

The best starting point to create organizational change toward achieving an AI-enabled workforce would be to start with the education and training for leadership and acquisitions. This level of education should also be combined with realistic experimentation exercises and wargaming on how to employ pro-

posed or possible AI-enabled systems. Some of this occurs already with XVIII Airborne Corps' AI-enabled live fire exercises and Army Future Command's Future Study Program.²⁴ Additionally, it is critical for the acquisitions personnel, who are responsible for "buying" all the AI-enabled technology, to obtain AI-enabled systems that can both meet warfighter needs and be used and maintained by Servicemembers. After that, as AI-enabled technologies begin to be distributed across the force, it will be important to prioritize user-level and maintenance-level training. Finally, while most of the examples in this article come from an Army perspective, the model and its associated roles and observations should generally apply to any military Service.

A key component of a revolution in military affairs is the ability of a military force to successfully incorporate new technologies into operations, training, doctrine, and other military processes.²⁵ The advantages of AI will come to the military that can best employ it.²⁶ To realize the potential groundbreaking value of AI technology, military organizations must work toward creating an AI-enabled workforce. The creation of this workforce should be based on the nature of AI in the military rather than an obsession with expertise or defaulting to AI experts due to lack of knowledge about AI. As such, I advocate for an AI skills-in-depth model that decreases focus on creating AI experts, which is both costly and—given integrated AI warfighting has not fully arrived—not yet necessary en masse, as their skills would just atrophy. Creating an AI-enabled workforce requires more than just training AI experts and hoping AI will deliver revolutionary effects on the battlefield. **JFQ**

Notes

¹ *Final Report* (Washington, DC: National Security Commission on Artificial Intelligence, 2021), 119–131, <https://www.nsc.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.

² Michael Raska and Richard Bitzinger, "Artificial Intelligence: A Revolution in Military

Affairs?" Singapore Defence Technology Summit, June 26–28, 2019, https://www.dsta.gov.sg/docs/default-source/documents/190625_tech-summit-commentary_a-revolution-in-military-affairs.pdf.

³ José-Marie Griffiths and Justin Lynch, "How to Build a Well-Rounded AI Workforce," *National Defense*, October 21, 2020, <https://www.nationaldefensemagazine.org/articles/2020/10/21/how-to-build-a-well-rounded-ai-workforce/>.

⁴ Diana Gelhaus and Santiago Mutis, *The U.S. AI Workforce: Understanding the Supply of AI Talent*, CSET Issue Brief (Washington, DC: Center for Security and Emerging Technology, January 2021), <https://cset.georgetown.edu/publication/the-u-s-ai-workforce/>.

⁵ Griffiths and Lynch, "How to Build a Well-Rounded AI Workforce"; Joe Chappa, "Trust and Tech: AI Education in the Military," *War on the Rocks*, March 2, 2021, <https://warontherocks.com/2021/03/trust-and-tech-ai-education-in-the-military/>.

⁶ Marianne Bellotti, "Helping Humans and Computers Fight Together: Military Lessons from Civilian AI," *War on the Rocks*, March 15, 2021, <https://warontherocks.com/2021/03/helping-humans-and-computers-fight-together-military-lessons-from-civilian-ai/>.

⁷ Veljko Kronic, *Succeeding with AI: How to Make AI Work for Your Business* (New York: Manning, 2020).

⁸ D. Sculley et al., "Hidden Technical Debt in Machine Learning Systems," Conference and Workshop on Neural Information Processing Systems, 2015, <https://proceedings.neurips.cc/paper/2015/file/86df7dcfd896fcdf2674f757a2463eba-Paper.pdf>.

⁹ Zachary S. Davis, *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise* (Livermore, CA: Center for Global Security Research, Lawrence Livermore National Laboratory, 2019), https://cgsl.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf.

¹⁰ Keith Jordan, "All Together Now," U.S. Army, August 20, 2014, https://www.army.mil/article/132125/all_together_now.

¹¹ Marigold Black et al., *Supporting the Royal Australian Navy's Campaign Plan for Robotics and Autonomous Systems: Human-Machine Teaming and the Future Workforce* (Canberra: RAND Australia, 2022), chap. 3, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1377-2/RAND_RRA1377-2.pdf.

¹² Eric Holder, email correspondence with author, July 2021.

¹³ *DOD AI Education Strategy: Cultivating an AI Ready Force to Accelerate Adoption* (Washington, DC: Joint Artificial Intelligence Center, 2020), https://www.ai.mil/docs/2020_DoD_AI_Training_and_Education_Strategy_and_Infographic_10_27_20.pdf.

¹⁴ Griffiths and Lynch, "How to Build a

Well-Rounded AI Workforce."

¹⁵ Bruce Nagy, "Tips for CDRLs/Requirements When Acquiring/Developing AI-Enabled Systems," Proceedings of the Nineteenth Annual Acquisition Research Symposium, May 2, 2022, <https://dair.nps.edu/bitstream/123456789/4587/1/SYM-AM-22-074.pdf>.

¹⁶ Army Futures Command, "Recruiting Window Now Open for Next AFC Software Factory, Cloud Technician Cohorts," U.S. Army, June 7, 2021, https://www.army.mil/article/247292/recruiting_window_now_open_for_next_afc_software_factory_cloud_technician_cohorts.

¹⁷ *DOD AI Education Strategy*.

¹⁸ Harshit Tyagi, "What Is MLOps—Everything You Must Know to Get Started," *Towards Data Science*, March 25, 2021, <https://towardsdatascience.com/what-is-mlops-everything-you-must-know-to-get-started-523fd0b8bd8>.

¹⁹ Alexandra Farr and Bre Washburn, email correspondence with author, February 2022.

²⁰ "CMU Partners with U.S. Army To Grow Data Science and AI Expertise," Carnegie Mellon University, September 1, 2020, <https://www.cmu.edu/news/stories/archives/2020/september/army-partners-grow-data-science.html>.

²¹ "DAF-MIT AI Accelerator," Department of the Air Force and Massachusetts Institute of Technology, 2023, <https://aia.mit.edu/>.

²² *Final Report*, 119–131.

²³ Griffiths and Lynch, "How to Build a Well-Rounded AI Workforce."

²⁴ Dan Roper, "Special Edition: Army Future Study Program," interview with Stephanie Ahern and Jean Vettel, Association of the United States Army's *Army Matters* podcast, March 29, 2021, <https://podcast.ousa.org/e/special-edition-army-future-study-program/>.

²⁵ Williamson Murray and Macgregor Knox, "Thinking About Revolutions in Warfare," in *The Dynamics of Military Revolution, 1300–2050*, ed. Macgregor Knox and Williamson Murray (Cambridge: Cambridge University Press, 2001), 175–194.

²⁶ Paul Scharre, *Robotics on the Battlefield—Part 1: Range, Persistence, and Daring* (Washington, DC: Center for a New American Security, May 2014), https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS_RoboticsOnTheBattlefield_Scharre.pdf?mtime=20160906081925&focal=none.



Professor Leigh Caraher, director of Applied Communication and Learning Lab, U.S. Army War College, participates as one of 29 professional military education faculty judges for SECDEF and CJCS Essay Competitions, hosted by NDU Press, Fort McNair, Washington, DC, May 12, 2023 (NDU Press)

Enhancing National Security

Increasing Female Faculty in Professional Military Education Would Strengthen U.S. Security

By Magdalena Bogacz

The relationship between national security and professional military education (PME) is long-standing. Traditionally, PME institutions

were established to do two things: to better prepare future leaders of the United States and select allies to overcome multidimensional threats to the apparent well-being of their people, and to sharpen the U.S. military's competitive edge. Both functions are essential to national security. Hence, PME institutions play an integral role in pre-

serving the Nation's physical integrity and territory as well as protecting and defending its citizens.

However, as some scholars have noted, PME experiences a persistent problem: "the counterproductive 'sea of sameness.'"¹ PME is dominated by men, just like the military and majority of academia. In fact, women, on average,

Dr. Magdalena Bogacz is an Assistant Professor of Leadership and Ethics in the Global College of PME at Air University.

occupy only 10 percent to 15 percent of all faculty positions at Army, Marine Corps, Navy, and Air Force PME institutions.² Gender disparity is even more pronounced at the senior Service schools. This is to say that there is a slightly higher percentage of women faculty in primary developmental education schools, but the number decreases as the level of education increases, with the fewest women faculty in senior developmental education schools such as the Air War College or Army War College.

Gender gaps in and of themselves are not problematic; there is nothing intrinsically wrong with having an unequal gender distribution among different professions. In fact, some researchers argue that it is in our nature to have different interests and thus pursue different occupations and domains of life.³ This view, called the gendered-interests hypothesis, could potentially explain away the root cause of gender imbalance in some academic disciplines. Hence, although female underrepresentation in PME is not necessarily a sign of gender discrimination, gender bias, or stereotype threat, and might in fact have come about by women's autonomous decisions to stay away from the field, it is important to consider the implications of such severe gender imbalance for the quality of education that these institutions provide as well as the subjective conditions in which they produce new knowledge.

The collective intelligence of any academic community comes from heterogeneity of its members—from exposure to the free exchange of ideas, mix of personalities, disagreements, and variance in demographic and social backgrounds. Moreover, diversity of thoughts and perspectives could, in principle, provide more creative and objective working environments.⁴ Thus, PME with such a small percentage of women instructors is at best limited in scope, because it eliminates a variety of different perspectives, and at worst unreliable, because it produces limited knowledge. There might be truths to which national security will have no access unless PME increases the diversity of instructors' experiences.

For example, female academics make it easier to understand women in war, female peacekeepers, violence against women, and women who are political leaders, as well as the perspectives of the U.S. allies and partners that have a "feminist foreign policy."⁵ Moreover, female academics would contribute to a better understanding of peace negotiations and peace agreements; "women's perspectives and participation, which are vital to achieving and sustaining peace, are too often overlooked in conflict resolution, prevention, and relief and recovery efforts."⁶ There is an established and robust correlation between peace agreements signed by female delegates and durable peace.⁷ In fact, United Nations data from the analysis of 40 peace processes since the end of the Cold War shows that "in cases where women were able to exercise a significant influence on the negotiation process, there was a much higher chance that an agreement would be reached than when women's groups exercised weak or no influence."⁸ Moreover, women's participation in a peace agreement, in and of itself, increases the probability of that agreement's lasting at least 2 years by 20 percent and lasting 15 years by 35 percent.⁹ Hence, without an increased number of female academics, knowledge discovery and knowledge building, as they relate to peace, negotiations, and leadership, will remain impaired.

Advancing inclusion of women in PME as it pertains to faculty representation will better equip both military and national security to adapt to a socially and demographically changing world. The remainder of this article explicates military homogeneity, including the gender gap in PME, then explains the significance of women's underrepresentation in PME. Next, it makes the case that increasing participation of women in PME would strengthen national security by strengthening the knowledge produced and providing a more comprehensive picture of the security environment. Finally, it discusses barriers to faculty diversity and provides an evidence-based list of hiring and retention practices that would help ensure that the best women apply to and stay at PME institutions.

Military Homogeneity and Lack of Faculty Diversity in PME

Although women have played a role in national security since the Revolutionary War, Brenda Oppermann refers to the process of their integration in the U.S. military as a "perennial struggle."¹⁰ Undeniably, progress has been made. Oppermann lists five events that played a critical role in advancing women's inclusion in military operations:

- passing the Women's Armed Services Integration Act
- passing Public Law 94-106, which allowed women to attend service academies
- repealing the Direct Ground Combat Definition and Assignment Rule (often referred to as the Combat Exclusion Rule)
- conducting combat operations in Iraq and Afghanistan
- implementing the U.S. National Action Plan on Women, Peace, and Security.

Oppermann suggests that the first three events helped with integrating women into the Armed Forces, whereas the last two highlighted the importance of gender perspective, which turned out to be indispensable in military operations.

Public Law 94-106, authorizing women to attend Service academies, passed in 1975. Since then, women's admission to military academies has meant that they are able to receive the most prestigious education alongside their male counterparts and, more important, can finally assume military leadership positions in significant numbers. A similar evolution affected female academics. However, although Public Law 94-106 passed 48 years ago, women continue to be underrepresented in a vast majority of PME institutions. For example, recent demographics data indicates that 14,536 civilians work for the Air Education and Training Command (AETC), one of the nine major commands of the Air Force (USAF) reporting directly to USAF Headquarters. The primary mission of AETC, which was established in 1993 by combining Air Training Command and

Air University, is to “recruit, train, and educate Airmen to deliver air power for America.”¹¹ Among the civilians working for AETC, 69 percent are men, and 70 percent of these men are Caucasian. This means that about 4,506 female civilians work for AETC. Moreover, less than 2 percent of the civilian workforce have a doctorate, and only about 20 percent have a master’s degree.¹² Since most faculty positions at PME institutions require a master’s degree (but strongly prefer a Ph.D.), it can be reasonably inferred, based on data from various PME institutions, that the percentage of civilian female faculty with a Ph.D. at AETC is significantly less than 15 percent.¹³

In the past, almost 10 percent of academics at the Naval War College were women, but this number has steadily declined, with 9 women having left since 2021. Of the 99 faculty and staff members at Marine Corps University, only 15 are women. Moreover, the numbers fluctuate depending on the level of education. For instance, primary education schools, such as the Squadron Officer School at Air University, generally have more women faculty than senior-level education schools. The Air Command and Staff College currently has 105 faculty members, 11 of whom are women, while Air War College has only 3.¹⁴

The situation of women in PME is reflective of academia as a whole. Numerous studies demonstrate that women have been underrepresented, underrated, and underrewarded in most academic disciplines for decades.¹⁵ Some fields, however, are more gender-imbalanced than others. For instance, the extreme underrepresentation of women in science, technology, engineering, and mathematics fields and occupations is well documented.¹⁶ Such gender disparities permeate academia and labor markets, as shown by various measures, from the number of students enrolled in undergraduate courses and the number of students earning degrees to the number of full-time faculty members and earning gaps.

Although significant progress has been made in terms of the visibility and advancement of women in some

academic fields, a severe gender imbalance persists in others.¹⁷ PME is one of the sectors that continue to have a large gender gap. As a result, women’s contributions to PME academics and scholarship are likely similar in scale to those of the initial wave of women entering colleges and universities about three decades ago.

Significance of Women’s Underrepresentation in PME. It is important to examine the gender gap in PME for a variety of reasons. As a result of gender inequity in the field, women and their scholarship are not fairly represented. Although women constitute a little over half of the total population of the United States, “they do not occupy half of all full-time university faculty positions, publish half of all academic journal articles, or constitute half of the highest social status members of academia.”¹⁸

Fields experiencing severe gender imbalance have been equated to a microcosm of the larger U.S. society, in which hierarchies arise from systemic discriminatory practices.¹⁹ If this is true, women’s underrepresentation in PME may be a result of systemic gender discrimination. And if so, then advancing inclusion of women as PME faculty is a matter of gender equality and fairness of organizational practices.

Nevertheless, women are not the only casualty of the gender gap in PME. The entire sector of military education also suffers negative ramifications. The lack of gender parity across PME programs and academic departments affects the way in which PME is executed nationwide. Knowledge produced under limited conditions (such as a lack of heterogeneity of thought or diversity of experiences) is conceivably less reliable than knowledge produced in a more inclusive and comprehensive environment. In addition, a field that is potentially influenced by implicit bias, stereotype threat, and gender discrimination may suffer from subjectiveness and thus be inclined to promote idiosyncratic ideas.²⁰ Finally, the relative lack of female faculty (and by extension, of their gender perspective) impairs adaptation to a changing world; today’s knowledge-based economies

require more comprehensive pictures of security environments, which cannot be generated without women’s perspectives. An understanding of the asymmetry of powers in patriarchal societies, gender prejudice and discrimination, feminist foreign policies, women in war, and women in the military is significantly diminished without the participation of female academics. Hence, the gender gap in PME may be a contributing factor to weakened national security.²¹ Therefore, it is necessary to move toward more gender-balanced faculty distribution for three significant reasons: fairness of organizational practices, the quality of PME, and enhanced national security.

Enhancing National Security by Increasing the Number of Women Faculty in PME. In their 2020 document titled *Developing Today’s Joint Officers for Tomorrow’s Ways of War*, the Joint Chiefs of Staff presented their new vision and guidance for PME.²² They called on education leaders to implement fundamental changes, where appropriate, to achieve intellectual overmatch against adversaries. The rapidly evolving security environment, the Joint Chiefs continued, requires changes in the character and conduct of warfare: “Our vision is for a fully aligned PME and talent management system that identifies, develops, and utilizes strategically minded, critically thinking, and creative joint warfighters skilled in the art of war and the practical and ethical application of lethal military power.”²³ This vision requires that our reimagined PME programs should rely more on innovation, creativity, original thought, and cutting-edge research to keep up with globalization, the return of Great Power competition, and the constantly changing character of war.

The dynamic and globally integrated environment requires a new and all-encompassing approach to teaching and learning. Such a new approach should, in principle, provide a more comprehensive learning experience and thus generate more comprehensive knowledge about the security environment. One way to generate a competent and exhaustive teaching and learning environment is by bringing in diverse talent. Educators



For first time in history of West Point, four current members of West Point faculty, from left, Colonels Julia Wilson, Kate Conkey, Julia Coxen, and Katie Matthew, have both commanded an Army battalion and earned a Ph.D., U.S. Military Academy at West Point, New York, March 27, 2023 (U.S. Army/Elizabeth Woodruff)

are supposed to challenge students, and a nondiverse faculty has less of a chance of challenging students. Moreover, by including more female voices, PME would increase its chances of gathering, assessing, analyzing, evaluating, and disseminating information in a more inclusive, global, and complete fashion.

Therefore, uneven gender distribution among PME faculty has negative effects on national security. Only by equally engaging women and men at the faculty level can we hope to satisfy the Joint Chiefs' wish to "maintain our competitive advantage and successfully prepare for emerging ways of war our Nation could face."²⁴ Advancing inclusion of women in PME is no longer optional. There are truths to which national security could have no access unless PME promoted female scholarship. Hence, diversifying faculty would deliver a blend of academic excellence, multidisciplinary expertise, and a more comprehensive picture of the security environment.²⁵

Barriers to Faculty Diversity. In the past few decades, many colleges and universities have embarked on a journey to

increase historically underrepresented minorities and women on their faculties. As a result, much has been published on best practices for improving faculty diversity in terms of recruitment and retention.²⁶ Yet most institutions remain homogenous, and men still assume disproportionately more academic leadership positions than their female counterparts.

There are complex hurdles to faculty diversity. For instance, several scholars have noted five important barriers:

- the "pipeline" challenge
- outdated faculty recruitment and retention practices
- faculty diversity myths that abound in higher education
- the decentralized administrative culture of the academy
- the view that faculty diversity is incompatible with academic excellence.²⁷

In terms of the gender gap among faculty, I would add two more obstacles that specifically impede women's progress in academia: historical barriers that kept

women away from education for centuries, and current challenges that women face in academia, such as gender discrimination, gender bias, and stereotype threat. To overcome these challenges and increase the number of female faculty at PME institutions, our efforts should focus equally on hiring and retention practices. We need to search for, onboard, and keep the best possible women faculty members by updating our hiring and retention practices and creating an organizational culture and day-to-day work environment that will make women want to come to and stay at PME schools.

Richard Clark and Fred Estes have identified three influences responsible for organizational goal achievement: knowledge, motivation, and organizational resources.²⁸ According to these authors, organizational performance goals can be analyzed in terms of gaps. Gap analysis delineates an organization's performance goals and then determines gaps between the organization's current and desired achievement of those goals. Hence, to meet the goal of more gender-balanced



Brigadier General Linell A. Letendre, Dean of Faculty, delivers remarks to Class of 2022 at Graduation Ceremony at Air Force Academy, Colorado Springs, Colorado, May 25, 2022 (U.S. Air Force/Justin R. Pacheco)

faculty distribution, PME hiring committees require appropriate knowledge, motivation, and organizational resources.

Lack of knowledge and skills constitutes one of the three major causes of performance gaps. To be effective, organizations and performers need to know what their performance goals are and how to achieve them. Because people are frequently unaware of their own lack of knowledge and skills, it is important for them to be able to reflect on their potential knowledge and skills gaps and actively work toward closing them before, or while, attempting to accomplish their goals. Thus, PME hiring committees need to know about gender gaps in PME as well as understand historical barriers that have kept women from entering PME. They also need to possess adequate skills to successfully implement diversity-oriented hiring and retention practices, all while actively reflecting on their own gender biases.²⁹

In addition to knowledge, another key influence on performance is *motivation*, defined as “the process whereby goal-directed activity is instigated and sustained.”³⁰ This definition suggests that motivation can be measured by

three factors: active choice to pursue a given action, degree of involvement, and persistence.³¹ Motivation is innately cultural: “We develop motivational beliefs from others with whom we interact in the variety of social contexts in the ecological niches we inhabit.”³² Thus, motivation is context-specific and depends on the dynamic interplay of internal (beliefs and perceptions) and external (sociocultural and organizational) factors. PME hiring committees need to be self-motivated to reach the goal of hiring more women faculty. Hiring committee members must recognize diversity as important and valuable in and of itself. In addition, they should feel confident in their abilities to implement the necessary measures, such as gender-equitable hiring practices, to successfully reach organizational goals. Confidence in one’s ability to reach a certain goal has been called self-efficacy, and it can be individual or collective.³³ I suggest that hiring committee members require both individual and team confidence in possessing necessary knowledge and skills to fulfill their recruiting duties correctly and efficiently.

Organizational influences are the final performance factor. Organizational

culture and resources can be either barriers to or assets in reaching complex organizational goals. Researchers have divided organizational influences into two categories: cultural models and cultural settings.³⁴ *Cultural models* are an organization’s shared beliefs and values that define individuals’ attitudes and judgments, whereas *cultural settings* are manifestations of cultural models, such as policies, practices, resources, and people. The two are intertwined; organizational culture is a product of interactions between people and their work environment.³⁵ For those reasons, PME institutions should work toward developing a welcoming climate that is safe and supportive of women; the degree of success in doing so will affect the degree of their success in attracting and retaining more diverse faculty candidates. Consequently, to help hiring committees reach the goal of diversifying faculty in terms of gender, PME institutions should prioritize organizational change by promoting a culture of inclusivity. One method of doing so involves having effective role models in leadership positions, who set high expectations regarding faculty diversity and provide

top-down support, such as effective hiring infrastructure, financial resources, and professional development opportunities for hiring committees' members.

Promising Practices for Increasing Female Faculty in PME

High-performing organizations have been defined as “organizations which are highly responsive to the customer, bring value to all stakeholders (employees, customers, suppliers, shareholders etc.); continuously improvise their processes, products and give better financial results on consistent basis in comparison to their competitors.”³⁶ Analysis of this definition provides us with a few key characteristics of high-performing organizations: employees with a high level of individual initiative, high productivity and innovation, aligned performance goals, and effective leadership.³⁷ To translate these key characteristics to a PME setting means understanding PME in terms of its core values. The Joint Chiefs' new vision for PME encourages educational leaders to transform our current system: “The profound and rapidly changing character of war and conflict in the 21st century compels us to transform our leader development to maintain our competitive advantage and successfully prepare for the emerging ways of war our Nation could face.”³⁸ If PME's purpose is to produce the strong and ethical leaders needed by the Nation, then PME's goals must align with national security goals. And developing adaptive and effective joint warfighters, and thus enhancing the security environment, is possible only if PME itself adapts to the fast-changing world. We must tackle emerging intellectual requirements to continue having a strategic military advantage over our adversaries. As the Joint Chiefs put it, “We must consistently prioritize critical and creative thinking, continuous learning and professional development, and the pursuit of transregional and cross-domain excellence in the development and assignment of joint warfighters.”³⁹

To achieve this blend of excellence and cross-domain expertise, PME needs

to hire more women. What follows is a short list of evidence-based gender-equitable hiring and retention practices derived from my earlier work. These faculty recruitment and retention strategies have been shown to be promising in attracting, hiring, and keeping a more diverse pool of faculty.

Research on how to close the gender gap in academic fields that have historically excluded women from participation has found that there are several promising practices that can increase the number of women who apply to and choose to stay in academic departments that are dominated by men.⁴⁰ Hiring best practices include use of intentional and diversity-oriented language in job advertisements, deliberate efforts to recruit broadly and advertise inclusivity and diversity, and spousal hiring. The best retention practices comprise a shared commitment to achieving diversity of views, backgrounds, and experiences and creating a family-friendly environment.

PME's ability to hire the best female candidates would increase if more time and effort were invested in using intentional and diversity-oriented language in job advertisements. Each position description should be crafted with language that appeals to underrepresented populations and should contain a note on PME's ongoing commitment to diversity and inclusion efforts. Moreover, PME should seek candidates who work between different areas and create bridges to other disciplines; interdisciplinary study in and of itself promotes diversity of thought and research. Furthermore, PME should put deliberate effort into recruiting women broadly. Job postings should be sent to often overlooked places of recruitment that are known to have large numbers of qualified women candidates. Ultimately, PME should try to share job postings with as many candidates as possible to ensure that they reach nonstandard channels of recruitment and increase the chance of attracting historically marginalized populations. Diversifying a pool of initial candidates is important; it increases the chance of getting the best woman for the job. And finally, to hire more women, PME

should consider offering spousal hiring. Statistically, women who belong to the academy are more likely to be partnered with another academic than their male counterparts.⁴¹ Institutions that offer spousal hiring as part of their gender-equitable hiring practices are more likely to attract women applicants.

In terms of retention, two practices in particular have proved effective.⁴² The first is a shared commitment to achieving diversity in views, backgrounds, and experiences. PME's organizational culture should insist on working toward making women feel equal to their male counterparts. Creating a culture that is welcoming and safe for women is one of the best methods to retain them in the sector. Women and their viewpoints need to be given the same amount of respect and attention as we see PME giving men and their ideas. Only with equal acknowledgment will women stop feeling like the other, the outsider, the second-class-citizen faculty. Besides committing to a culture that actively addresses historical exclusion of women, PME should focus on showcasing family friendliness. This organizational culture feature is especially important for retaining women for the long term. Female academics' careers are disproportionately affected by childbearing and childcare. PME may need to consider special accommodations to level the playing field between female faculty and their male counterparts, such as flexible schedules and a gender-neutral parental leave policy.

This article argues that to enhance national security, PME must focus on hiring and retaining more female faculty. The status of our nation's security depends largely on the status of women in PME. Women provide diversity of thought that is otherwise unachievable; the gender perspective that female faculty provide is critical in developing our joint warfighters for tomorrow's ways of war. As a result, to enhance national security, we must focus on broadening our educational perspectives by recruiting the best female academics. Without increasing the number of women in PME, the United States is failing to maximize its potential success in national security. JFQ

Notes

¹ Joan Johnson-Freese, Ellen Haring, and Marybeth Ulrich, "The Counterproductive 'Sea of Sameness' in PME," *Joint Force Quarterly* 74 (3rd Quarter 2014), 58–64, <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-74/Article/577529/the-counterproductive-sea-of-sameness-in-pme/>.

² Exact statistics about the number of female professional military education (PME) faculty were difficult to compile. I gathered data from different primary-, intermediate-, and senior-level Service schools' Web sites and from faculty at different PME institutions. As a reference point, I also used Johnson-Freese, Haring, and Ulrich, "The Counterproductive 'Sea of Sameness' in PME."

³ Tom Dougherty, Samuel Baron, and Kristie Miller, "Female Under-Representation Among Philosophy Majors: A Map of the Hypotheses and a Survey of the Evidence," *Feminist Philosophy Quarterly* 1, no. 1 (2015), <https://ojs.lib.uwo.ca/index.php/fpq/article/view/2984>; Stacey Goguen, "Is Asking What Women Want the Right Question? Underrepresentation in Philosophy and Gender Differences in Interests," *Dialogue; Canadian Philosophical Review/Revue canadienne de philosophie* 57, no. 2 (June 2018), 409–441; Morgan Thompson et al., "Why Do Women Leave Philosophy? Surveying Students at the Introductory Level," *Philosophers' Imprint* 16, no. 6 (March 2016), 1–36, <https://quod.lib.umich.edu/p/phimp/3521354.0016.006/1>.

⁴ Damon Williams, *Strategic Diversity Leadership: Activating Change and Transformation in Higher Education* (Sterling, VA: Stylus Publishing, 2013); Damon Williams and Katrina Wade-Golden, *The Chief Diversity Officer: Strategy, Structure, and Change Management* (Sterling, VA: Stylus Publishing, 2013).

⁵ Joan Johnson-Freese, *Women, Peace, and Security: An Introduction* (New York: Routledge, 2019).

⁶ "Promoting Gender Equality and Advancing the Status of Women and Girls," Department of State Fact Sheet, September 8, 2014, <https://2009-2017.state.gov/r/pa/pl/231391.htm>.

⁷ Jana Krause, Werner Krause, and Piia Branfors, "Women's Participation in Peace Negotiations and the Durability of Peace," *International Interactions* 44, no. 6 (2018), 985–1016, <https://www.tandfonline.com/doi/full/10.1080/03050629.2018.1492386>.

⁸ Marie O'Reilly, Andrea Ó. Súilleabháin, and Thania Paffenholz, "Women's Participation and a Better Understanding of the Political," in *A Global Study on the Implementation of United Nations Security Council Resolution 1325* (December 2022), <https://wps.unwomen.org/pdf/CH03.pdf>.

⁹ Ibid.

¹⁰ Brenda Oppermann, "Women and

Gender in the U.S. Military: A Slow Process of Integration," in *Women and Gender Perspectives in the Military*, ed. Robert Egnell and Mayesha Alam (Washington, DC: Georgetown University Press, 2019).

¹¹ "AETC Snapshot," Air Education and Training Command, 2020, [https://www.aetc.af.mil/Portals/88/Documents/Snapshot/AETC Snapshot FY20 April 7 2021.pdf](https://www.aetc.af.mil/Portals/88/Documents/Snapshot/AETC%20Snapshot%20FY20%20April%207%202021.pdf).

¹² Ibid.

¹³ Air War College Web site, "Leadership and Faculty," November 2022, <https://www.airuniversity.af.edu/AWC/Leadership-and-Faculty/>; Army War College Web site, "Faculty Directory," November 2022, <https://ssl.armywarcollege.edu/faculty/#/facultyCouncilList>; Naval War College Web site, "Faculty and Departments Directory," February 2022, <https://usnwc.edu/Faculty-and-Departments/Directory>.

¹⁴ Ibid.

¹⁵ *The Annual Report of the Economic Status of the Profession, 2018–19* (Washington, DC: American Association of University Professors, 2019), https://www.aaup.org/sites/default/files/2018-19_ARES_Final_0.pdf.

¹⁶ Scott A. Ginder, Janice E. Kelly-Reid, and Farrah B. Mann, *Integrated Postsecondary Education Data System Methodology Report 2013–14* (Alexandria, VA: National Center for Education Statistics, 2014).

¹⁷ Abigail J. Stewart and Virginia Valian, *An Inclusive Academy: Achieving Diversity and Excellence* (Cambridge, MA: MIT Press, 2018).

¹⁸ Eric Schwitzgebel and Carolyn Dicey Jennings, "Women in Philosophy: Quantitative Analyses of Specialization, Prevalence, Visibility, and Generational Change," *Public Affairs Quarterly* 31, no. 2 (April 2017), 83.

¹⁹ Cecilia L. Ridgeway, *Framed by Gender: How Gender Inequality Persists in the Modern World* (New York: Oxford University Press, 2011).

²⁰ Jennifer Saul, "Implicit Bias, Stereotype Threat, and Women in Philosophy," in *Women in Philosophy: What Needs to Change?* ed. Katrina Hutchison and Fiona Jenkins (New York: Oxford University Press, 2013).

²¹ Joan Johnson-Freese, "Gender Equality as a Security Issue," *YaleGlobal Online*, September 17, 2019, <https://archive-yaleglobal.yale.edu/content/gender-equality-security-issue>.

²² *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education & Talent Management* (Washington, DC: The Joint Staff, 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817.

²³ Ibid., 2.

²⁴ Ibid., 1.

²⁵ Statement of Kayla Williams, *Increasing Diversity in the Military: Recruiting and Retaining Talented Women*, Testimony Before the Subcommittee on Military Personnel, House

Armed Services Committee, 116th Cong., 1st sess., December 10, 2019, <https://www.jstor.org/stable/resrep28746>.

²⁶ Aldamero Romero, Jr., *Best Practices for Recruiting and Retaining Diverse Faculty for Institutions of Higher Education* (New York: CUNY Academic Works, 2017), [https://www.ccas.net/files/public/Publications/Best Practices CCAS_March 2017_FINAL.pdf](https://www.ccas.net/files/public/Publications/Best%20Practices%20CCAS_March%202017_FINAL.pdf).

²⁷ Williams and Wade-Golden, *The Chief Diversity Officer*, 282.

²⁸ Richard E. Clark and Fred Estes, *Turning Research Into Results: A Guide to Selecting the Right Performance Solutions* (Charlotte, NC: Information Age Publishing, 2008).

²⁹ Ibid.

³⁰ Dale H. Schunk, Judith R. Meece, and Paul R. Pintrich, *Motivation in Education: Theory, Research, and Applications* (New York: Pearson, 2009), 4.

³¹ Helena Seli and Myron H. Dembo, *Motivation and Learning Strategies for College Success: A Focus on Self-Regulated Learning*, 6th ed. (New York: Routledge, 2019).

³² Robert Rueda, *The 3 Dimensions of Improving Student Performance: Finding the Right Solutions to the Right Problems* (New York: Teachers College Press, 2011), 39.

³³ Frank Pajares, "Overview of Social Cognitive Theory and of Self-Efficacy," n.d., <http://people.wku.edu/richard.miller/bandurathory.pdf>.

³⁴ Ronald Gallimore and Claude Goldenberg, "Analyzing Cultural Models and Settings to Connect Minority Achievement and School Improvement Research," *Educational Psychologist* 36, no. 1 (2001), 45–56.

³⁵ Ibid.; Clark and Estes, *Turning Research Into Results*.

³⁶ Kapil Pandla, "Drivers and Characteristics of High Performing Organizations," *International Journal of Business and Administrative Studies* 2, no. 3 (June 2016), 78–82.

³⁷ Marc J. Epstein, "The Drivers and Measures of Success in High Performance Organizations," in *Performance Measurement and Management Control: Superior Organizational Performance*, ed. Marc J. Epstein and Jean-François Manzoni, *Studies in Managerial and Financial Accounting*, vol. 14 (Amsterdam: Elsevier, 2014).


³⁸ *Developing Today's Joint Officers for Tomorrow's Ways of War*, 1.

³⁹ Ibid., 3.

⁴⁰ Magdalena Bogacz, "Gender Parity in American Academic Philosophy: A Promising Practice Study" (Ph.D. diss., University of Southern California, August 2021), <https://rossier.usc.edu/documents/bogacz-magdalena-2021>.

⁴¹ Londa Schiebinger, Andrea Davies Henderson, and Shannon K. Gilmartin, *Dual-Career Academic Couples: What Universities Need to Know* (Stanford: Stanford University, 2008).

⁴² Bogacz, "Gender Parity in American Academic Philosophy."



Falcon 9 rocket carrying 56 broadband satellites launches from Space Launch Complex 40 at Cape Canaveral Space Force Station, Florida, May 4, 2022 (U.S. Space Force/Joshua Conti)

Why Military Space Matters

By Gregory Gagnon

Militaries fight wars and, in times of peace, prepare for the next war. How they prepare matters. Preparing for war can help prevent war from breaking out. At the same time, militaries that prepare to fight the last war often fail in the next.

Over the past two-plus decades of military operations, our nation's ability to use outer space has not been consequentially challenged or contested. An unintended byproduct of that circumstance is we have

unintentionally conditioned strategists and national security professionals to assume the space advantage is our birthright. The Taliban didn't use space, the Iraqi Republican Guard didn't use space, and the so-called Islamic State (IS) didn't have any real way of challenging our space capabilities. In fact, in our past wars our adversaries didn't need to leverage space to fight and certainly had more important military objectives than attacking U.S. space capabilities. But if the next war is against a near-peer competitor, that will not be the case.

Space advantage is felt locally within ground, air, and naval force formations. The Taliban, IS, and Republican Guard

couldn't contest our use of space to disrupt joint operations. In the conflicts with them, integrating space from afar proved effective, but the challenge ahead is not the challenge of the past. The need to steadfastly integrate space capabilities and operations on tactical timelines into operational fires and to maneuver in what we expect to be a highly contested environment requires dedicated in-theater support.

The Chinese Communist Party's military, the People's Liberation Army (PLA), is planning both to leverage space capabilities to hold our allied forces at risk and to attack our ability to use space for military purposes. Space and cyberspace

Major General Gregory Gagnon, USSF, is Deputy Chief of Space Operations for Intelligence (S2).

are known as the “commanding heights” in China’s warfighting doctrine. The PLA intends to extend warfare into those domains. In fact, according to China’s 2019 defense white paper titled *China’s National Defense in the New Era*, the PLA Strategic Support Force (PLASSF) has “made active efforts to integrate into the joint operations systems. It has carried out confrontational training in new domains and trained for emergencies and combat.” This new PLA threat affects all facets of U.S. military planning. It is a change requiring the United States and our allies

to plan for and build forces to challenge and defeat PLA desires in space and cyberspace. Like cyberspace, space can be the great enabler of long-range fighting capabilities, or it can be the Achilles’ heel.

The PLA is not the Taliban. The PLA established the PLASSF 7 years ago to seek advantage from the changing character and complexity of warfare. The PLASSF comprises space, cyberspace, and electronic warfare forces. The integration of these functions enables the PLA to both modernize and advance intelligence-led, joint-power-projecting warfare. Last

year, China placed 200 satellites into orbit. Slightly more than 50 percent of these satellites conduct remote sensing, which can be used to gain intelligence on adversary military forces far from China’s shores. Moving into 2023, China had more than 700 operational satellites in space, indicating a 385 percent growth rate since the establishment of the PLASSF in December 2015. Today, these space activities are predominantly national security focused, supporting China’s goal of owning the “commanding heights.” On-orbit Chinese satellites



Army Major Mitchell Daugherty, mission director for National Space Defense Center, works with Space Force 1st Lieutenant Tia Scoggan, weapons and tactics section chief for 18th Space Defense Squadron Det. 1, at Schriever Space Force Base, Colorado, October 5, 2022 (U.S. Space Force/Tiana Williams)

are on average only 3 years old; it is the newest of technology, designed and built in our digital age.

The PLA's on-orbit intelligence infrastructure is a real and present danger. We have never faced a competitor with as much capability on orbit. Unlike the insurgents and terrorists, the PLA has a 21st-century space kit. Yes, it has satellites, but it also has space attack missiles, lasers, and even dual-use space robots that can be used to attack.

The United States and our allies must continue to focus on gaining and then maintaining the military advantage afforded by outer space for military operations. This has not been a necessary military task in the past.

Following the reorganization of the PLA and the establishment of the PLASSF, the United States established U.S. Space Command (USSPACECOM) and the U.S. Space Force (USSF), but not until late 2019. Our allies rapidly followed suit. In Europe, Germany, France, the United Kingdom, and Italy have all elevated Space Force organizations in their formations. In the Indo-Pacific, Japan, the Republic of Korea, and Australia have, as well. To our north, Canada established its first space wing in 2022. We all must use space capabilities to assist our ground, air, and naval forces to see farther, sense with greater clarity, and protect the joint force while operating at home and abroad. To do so, we must protect our space-enabled capabilities from defeat. We must be able to disable the adversary's ability to use space-enabled capability to its advantage in times of war to maximize protection of our fielded force.

Both USSPACECOM and USSF work collaboratively to achieve these goals with other organizations across the U.S. Government and with allies. Combatant commanders plan, direct, and assess joint operations for the Department of Defense. USSPACECOM works to ensure that we never have a day without military space advantage. USSF builds space forces that prepare for war and maintain readiness, and presents those forces to combatant commands to achieve space advantage. Additionally, the Navy and the Army train small cadres of specialized Servicemembers to integrate

space capabilities into ground and maritime operations. Furthermore, the USSF builds and presents the command and control capabilities necessary to synchronize joint operations in support of gaining and maintaining space advantage. This clarity of purpose did not exist prior to a separate space Service.

In the next war, should it occur, the complementary nature of USSPACECOM and USSF will prove crucial. Military space advantage in outer space is difficult to fragment; space operations are inherently holistic. Although a satellite can connect you to others or take an image, it may be overhead within direct sight for only minutes. Satellites move constantly. Currently, controlling satellites is best done with access points spread across the globe. This global nature of space operations helps explain why USSPACECOM has responsibilities that are worldwide, as well as above 100,000 feet. USSPACECOM has forces assigned from each of the military Services, although the vast majority come from the Space Force. Under the leadership of USSPACECOM, these forces are expected to deliver military advantage both in and from space. In short, they must ensure the ability to use outer space to deliver military effects at the time and place of our choosing.

Like USSPACECOM, combatant commanders across the globe will soon have a dedicated USSF component. The priority will initially be on the pacing challenge. We must prepare for an adversary with more surface combatants, more surface-to-air missiles, more military intelligence satellites, and more troops. We must prepare for a war very different from the battles of the last two decades. Strategists have long cautioned that militaries that fail to forecast changes in warfare tend to fail. For the United States and our allies, failure is not an option.

Our joint force must fully integrate space capabilities to optimize how we fight. The USSF space components to the combatant commanders will deliver and integrate cutting-edge space capabilities into land, sea, air, and cyberspace operations. At the same time, land, sea, air, and cyberspace operations will also be evolving. Soon, all Services will field advanced

capabilities that could impact outer space. As our potential adversaries' development has shown, advances in long-range fires, cyberspace capabilities, directed energy, and other capabilities are making the battlefield intensely multi-domain and spatially vast. The PLA has more jammers than any other military, including ours. The PLA has also fielded lasers for combat and is already training its space attack forces. The future operating environment will be contested, dangerous, and lethal over vast distances. The fight will also take place in space and cyberspace; it will be a multi-domain battle.

U.S. and allied planners must adjust to create fire-control synchronization and deconfliction elements and processes that account for allied multi-domain battles and an expansively deep "battlefield." Coordinating allied joint force weapons, deconflicting their impacts, and synchronizing operations back to USSPACECOM are critically important. In theater, USSF components should have this operational-level task levied on them by their respective joint combatant commanders. The USSF components should synchronize effects in support of theater terrestrial forces and support USSPACECOM's space maneuver and control objectives. This is new for space operations. In past wars, theater support was provisioned from afar and the relationship was one-directional: space support to ground ops. This process worked, but mainly because past adversaries were not space powers.

Space advantage is essential to U.S. power; it enables our forces to see with greater clarity, sense in the darkest of nights, and apply judicial precise force when directed. As we prepare for the next battle, we must accept that space advantage must now be gained. We must organize, prepare, and field combat-ready forces in all domains of warfare. These forces must also habitually train to fight together. These are unified actions, joint operations, and multi-domain operations. This is how we win a future war that will look very different from the wars of our recent past. And, if we organize and prepare for it, perhaps we'll never have to fight it. JFQ



Naval Aircrewman (Operator) 2nd Class Meghan Cooke, assigned to "Skinny Dragons" of Patrol Squadron (VP) 4, conducts flight operations aboard squadron P-8A Poseidon aircraft during intelligence, surveillance, and reconnaissance mission over Eastern Mediterranean Sea, near Sigonella, Sicily, March 20, 2020 (U.S. Navy/Juan Sua)

Improving Analytic Tradecraft

The Benefit of a Multilateral Foundational Training Model for Military Intelligence

By Eric Daniels

Professional builders know that the main purpose of a foundation is to secure the structure and keep it upright. A poorly constructed foundation can be dangerous to occupants and neighboring structures. Similarly, the

foundational training of our military intelligence professionals is paramount for our national security.

This training could be improved by soliciting the individual military Services by means of a multilateral approach. The Services should work together multilaterally through their lead commands for intelligence, versus unilaterally or even jointly, ensuring synchronized instruction at a foundational level. It is vital for the educational

framework that which, how, and when intelligence should be delivered to our military professionals in every Service be harmonized cohesively across strategic, operational, and tactical levels. Regardless of their specific roles within the profession, all Soldiers, Marines, Sailors, Airmen, and Guardians in the intelligence profession should have a solid understanding of the core analytic tradecraft standards that should apply to their daily work.

Eric Daniels is a U.S. Air Force Senior Intelligence Analyst with the 363rd Intelligence Surveillance Reconnaissance Wing under the Air Combat Command.

The Warning Light Flashed . . . Twice

The work that our military professionals do for the Nation is second to none. They are trained extensively in their designated fields as technicians first and analysts second, unlike their civilian intelligence community (IC) counterparts. More important, training in the military is taken seriously to ensure career development and to make certain every mission is accomplished with excellence.

The military intelligence profession is different from its counterparts in the civilian agencies. Nonetheless, it shares with them the requirement to keep classified information secure while providing unbiased, accurate reporting in a timely manner, which is both an art and a science. According to Intelligence Community Directive (ICD) 203, the intelligence provided to our military leaders must be objective, independent of political consideration, timely, and based on all available sources, and it must exhibit analytic tradecraft standards. This is where the issue resides: As a collective, the IC within the Department of Defense (DOD) has not met the required core principles of intelligence analysis across the entire IC.¹ The 2007 Intelligence Community Directive 203, *Analytic Standards*, lays the groundwork for the military's ability to govern the production and evaluation of analytic products and support intelligence professionals in striving for excellence, integrity, and rigor in their analytic thinking and work practices.

In 2010, Brigadier General Wayne Michael Hall, USA (Ret.), wrote:

These shortfalls in analytic training, education, and operations are not the fault of the courageous and talented people who perform analytic work today. It is, sadly enough, the defense institution's fault, as it has not yet engaged in the hard thinking work to first understand what is needed to support intelligence operations in urban settings, and then to set about to change intelligence analysis to produce thinking sufficient to go after insurgent, irregular warrior, and terrorist threats in large urban settings.²

In 2014, the first alarm sounded. The DOD Office of the Inspector General (DODIG) issued a report stating that

the DOD Intelligence Enterprise lacks intelligence training program standards for the common training needs and developmental skills. The military Services and agencies in the DOD Intelligence Enterprise each have varying processes for providing intelligence training and education to the intelligence workforce. As a result of the absence of DOD Intelligence Enterprise standards, the DOD developmental intelligence training program has a fragmented training structure, varying proficiency levels, training redundancy, and critical skill gaps.³

This report to Congress outlined the deficiencies in the DOD training structure as it pertains to intelligence functions such as human intelligence, geospatial intelligence, signals intelligence, and all-source intelligence.

Regardless of function, the DODIG reported that there is an issue with foundational training across the department. Whereas drastic improvements have been made in training standards on the joint level across the board by combat support agencies such as the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency, and the National Security Agency, on the operational and tactical levels, military Services still lack the momentum to stay on par with other agencies within their department. Whereas some would argue that the Service branches are meant to adapt to the battlespace and dynamic adversaries while the IC agencies can conduct more strategic analysis, others would suggest the absence of resources, specific policies, and other "organizational culture" issues continues to hamper the Service branches' momentum.⁴

Four years later, another warning was issued. In 2018, the DODIG issued a second report to Congress stating that

improvements are needed in the following areas in order to further support communications and analytical integrity. Specifically: Many military analysts lacked formal

training on ICD 203 Analytic Standards when they arrived at their commands. . . .

A majority of the military all-source intelligence analysts we interviewed had no prior training on ICD 203 Analytic Standards through other courses, and were not eligible to attend the DIA's PACE [Professional Analyst Career Education] training prior to 2018 DIA decisions to open the course to military personnel.⁵

This finding did not fall on deaf ears within the Services. Subsequently, many Services began using their own resources and methods to attempt to make improvements in their intelligence training. Still, the question remains: Are the Services' foundational intelligence training standards synchronized? Are the established elements within the Services and in the joint DOD actively playing a role to facilitate unity of effort to improve foundational training across the board? I would argue that a multi-lateral approach to improving training would provide each Service with the enhancements in tradecraft production that DOD desires. In addition, more rigorous production and a higher quality of analysis within the joint and Service components intelligence environment would be likely.

Let's Put Premium Tires on the Issue Instead of Reinventing the Wheel

The military should avoid reinventing the wheel. The practice of re-creating the wheel to stand up a new idea, fix problems, or simply ensure promotion is a little-discussed pet peeve in the community. Many mechanisms are already proposed in existing joint publications to help solve most if not all of the issues raised by the DODIG. One approach was to request that DIA's Joint Military Intelligence Training Center facilitate support in the military Services by opening its doors and providing instructors to train others besides its own agency's civilian and military analysts. Because of congressional funding lines, the request to provide direct support in various ways is being negotiated between DIA and military Service commands.

Air Force independent research, Navy publications, and Army intelligence brigade publications provide evidence backing the DODIG reporting and highlight the need for certified subject matter experts who have analytic experience on the strategic, operational, and tactical levels.⁶ As referenced in the 2018 DODIG report, the DIA PACE course (along with analytic certification requirements) has helped effect drastic improvements in analyst tradecraft standards across agencies. This finding indicates that improvements are possible within a year—the period from the initial warning to Congress. On the other hand, because of funding, allocation of resources, and other congressional mandates, the request to have DIA take the lead in this requirement is currently being negotiated.

Among some leaders across the Services, there is a misconception that analytic tradecraft standards are necessary only for strategic or possibly operational intelligence analysis. This is not true. Not only does ICD mandate these standards for all U.S. intelligence analysts, but also most Services mandate the use of these standards in their own regulations. What are the core issues that hinder foundational training for intelligence analysts across the Services to ensure our professionals are proficient analysts? Is it organizational culture? Is it funding? Is it a lack of knowledge? Why is the foundational training not synchronized across the board among the Services? Why are we not all speaking the same language when it comes to analytic production requirements by using the required ICD standards?

Some of these core issues can be solved multilaterally, through mechanisms already in place. Major James Kwoun, USA, an Active-duty intelligence officer, stated, “The prevailing view that tradecraft standards are applicable only at the strategic level is false. In fact, cognitive biases—one of the primary reasons for adopting analytic tradecraft standards—are arguably most prevalent at lower echelons.”⁷ There must be changes throughout the Services. The only way to begin messaging and see improvement across the Services in military analytic tradecraft is through foundational training

at the entry level. The approach needs to be synced multilaterally and requires a uniform training system that includes the U.S. Army Intelligence Center of Excellence (USAICoE), the Air Force Air Education and Training Command (AETC), and the Navy and Marine Corps Intelligence Training Center (NMITC). They must collaborate multilaterally to ensure that what they are teaching in their programs, and how and when they teach them, is harmonized. This does not mean it should be left to the joint world to solve their problems; the Services should continue their individual programs while simultaneously making sure those programs are synchronized to get the improvement needed.

Use a Wrench Instead of a Screwdriver to Change a Tire

The problem is clear: military Services’ foundational intelligence training standards are not sufficiently synchronized for DOD to fully meet analytic tradecraft standards. We have seen attempts to solve this problem in various ways, but the challenge of solving it without a large requirement of resources, time, and changes in policy remains. The DODIG recommended

*that the Under Secretary of Defense for Intelligence examine current DOD intelligence training and education policies and mandate, as necessary, training standards based on a common essential body of knowledge, including Intelligence Community Directive 203, “Analytic Standards,” January 2, 2015, for all entry-level and developmental intelligence professionals.*⁸

As previously stated, this recommendation was provided twice by DODIG, and the Services are currently “reinventing the wheel” to follow it. I would suggest the following multilateral approach.

Ways (Concept). USAICoE, AETC, and NMITC should extensively collaborate, coordinate, and communicate (three Cs method) at the Service level when it comes to formulating a course and syllabus and recruiting/selecting instructors who are Certified Defense All-Source Analysis (CDASA) 1–certified to teach

foundational courses that reinforce analytic tradecraft standards. This process should include collaborating through the existing DOD Intelligence Training and Education Board (DITEB) recommended in the 2014 DODIG report.⁹ This should be the central forum used by intelligence leaders in each Service, just as it would be if line analysts were working together to solve an analytic intelligence question. This is an opportunity to collaborate, coordinate, and communicate extensively to create a unified policy (product) that benefits the greater good for each Service and for national security. Using the three Cs method at the leadership level reinforces what is taught on a foundational level when it comes to the cornerstone of our craft.

Means (Resources). The Services should coordinate what they are teaching. The following should be congruent across the board when it comes to foundational analysis:

- A unified course, course syllabus, and course instruction methodology. Each Service currently has its own version of critical thinking, analytic writing, analytic tradecraft standards, and structured analytic techniques courses. These foundational courses should all be the same. Several reports have noted that Servicemembers deployed or assigned to a joint environment lack training in these foundational qualities; this lack affects their ability to work with civilian IC analysts who were taught at their respective agencies.¹⁰ Professionally, these courses are critical. Most if not all civilian IC agencies work together to ensure their material is synchronized, with the expectation that their analysts will work side by side in their career paths. They communicate effectively across agencies because of their foundational training. The Services should work together to ensure their courses use the same material and are taught the same way. The foundation of intelligence training *must* be synchronized across DOD.
- Incorporate CDASA 1–certified instructors. We want our elementary

school teachers, construction contractors, doctors, and accountants to be certified. Why do we require less when it comes to the instructors who teach the foundation of analysis to our intelligence professionals? According to the DOD CDASA program management office, “The development of professional certification programs ensures an integrated, agile intelligence workforce that can meet the department’s needs in a dynamic environment.”¹¹ CDASA-1 instructors understand the *Why?* the *What?* and the *So what?* and undoubtedly have the knowledge to teach foundational analytic skills. They have practical experience, have a breadth of knowledge in the area, and have successfully passed the qualifying exam. For each of the foundational requirements, we trust certified instructors to know what right looks like. Using such instructors would reinforce competence through training and support the DODIG recommendations of 2014 and 2018.

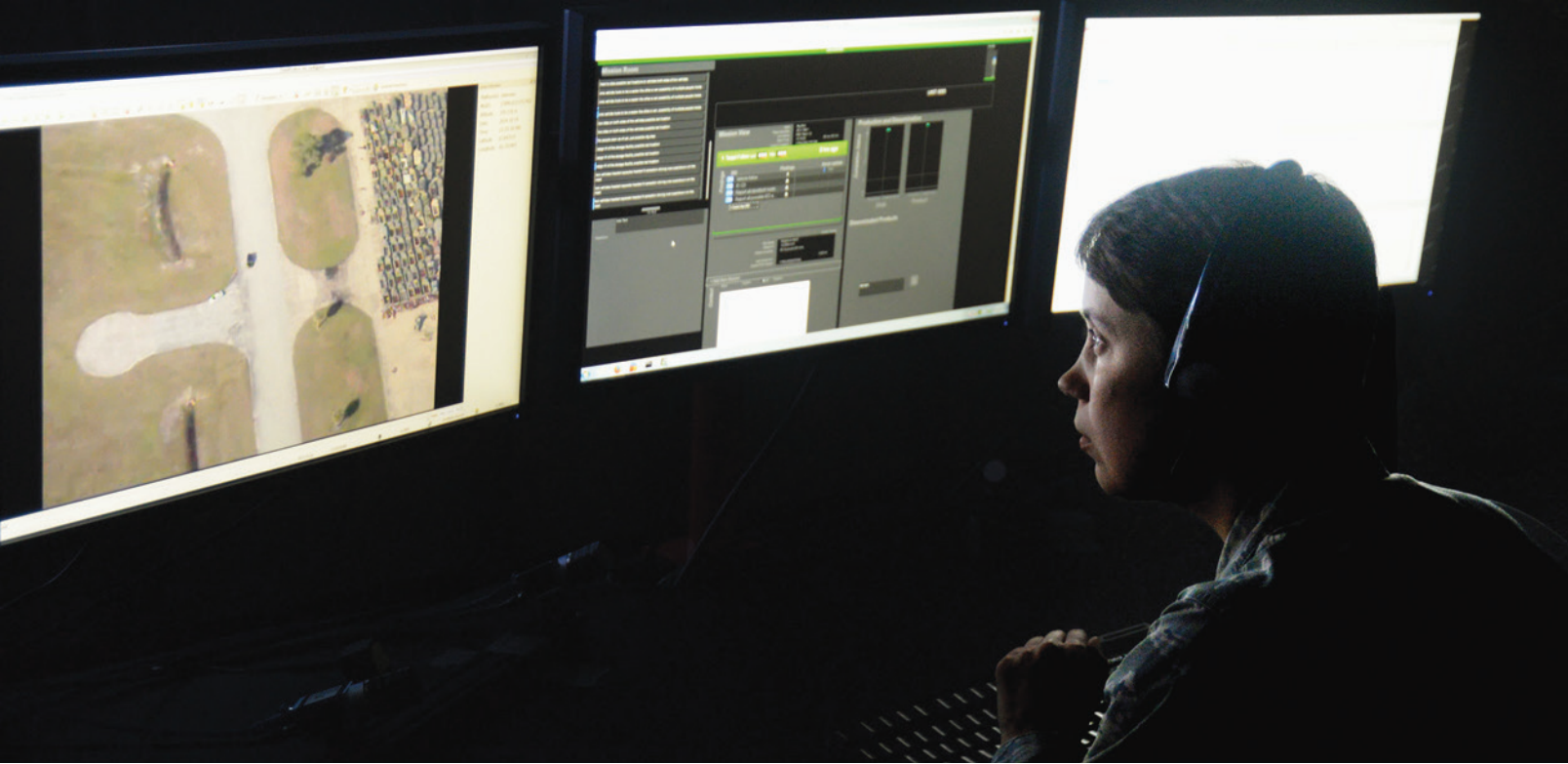
Ends (Objective). Through collaboration within the DITEB, each Service can better understand the rationale behind the recommended timing for each Service’s military occupational specialty requirements. As we know, each Service has its own training schools and programs for every occupational specialty. Most of them “rack and stack” their courses for different reasons. I would suggest that a small body of intelligence professionals, all with stakes in the matter, be selected to work together and create a three-Cs approach to make sure that all military intelligence professionals take foundational intelligence courses that include the same material at the same time in their careers.

Let’s Take a Walk Around the New Model and Be on Our Way to Success

There is no need for a new joint office to be constructed to solve this issue. Neither is there a need for major changes to be made in the bureaucracies within each military Service. Rather, we

need to teach intelligence tradecraft at a higher standard to solve foundational issues within the military Services that affect intelligence professionals. In 2010, Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor wrote, “Meaningful change will not occur until commanders at all levels take responsibility for intelligence. The way to do so is through devising and prioritizing smart, relevant questions—‘information requirements’—about the environment as well as the enemy.”¹² This quote hit the target, defining the solution to a clear risk to the foundation of our intelligence: excellence in training the Soldiers, Marines, Sailors, Airmen, and Guardians who conduct intelligence analysis and operations each day.

Conversely, consider the alternative: that the current intelligence training structures within each military Service should not consider syncing, instead just improving the intelligence training for the functional and geographic combatant commands. This alternative is possible,



Air Force 1st Lieutenant Amanda Chichester, 711th Human Performance Wing behavioral scientist, watches video loop for suspicious behavior during demonstration of new Enhanced Reporting, Narrative Event Streaming Tool developed by Air Force Research Lab, Wright-Patterson Air Force Base, Ohio, October 15, 2014 (U.S. Air Force/Wesley Farnsworth)

given that the 2014 and 2018 DODIG reports specifically recommended that the combatant commands make changes in their military analytic training policies and standards (and indeed these changes are already in progress). However, given military analysts' lack of training on ICD 203 standards, as noted in the 2018 DODIG report, sufficient progress on separate Service tracks seems unlikely.¹³

Implementing the DODIG recommendations under the auspices of already established programs and instituting multilateral approaches among the lead training centers within each Service center would support military commanders' and political leaders' confidence in military intelligence analysis across the board. JFQ

Notes

¹ Intelligence Community Directive 203, *Analytic Standards* (Washington, DC: Office of the Director of National Intelligence, January 2, 2015), <https://fas.org/irp/dni/icd/icd-203.pdf>.

² Wayne Michael Hall and Gary Citrenbaum, *Intelligence Analysis: How to Think in Complex Environments* (Santa Barbara, CA: Praeger Security International, 2009), 3, <https://publisher.abc-clio.com/9780313382666/20>.

³ Department of Defense Office of Inspector General (DODIG)-2015-015, *Evaluation of DOD Intelligence Training and Education Programs for the Fundamental Competencies of the DOD Intelligence Workforce* (Washington, DC: DODIG, October 31, 2014), I, [https://media.defense.gov/2018/Aug/31/2001960960/-1/-1/1/DODIG-2015-015 \(REDACTED\). PDF](https://media.defense.gov/2018/Aug/31/2001960960/-1/-1/1/DODIG-2015-015%20%28REDACTED%29.PDF).

⁴ M. Grunwald, M. Crouse, and R. Sullivan, "The State of Analysis and Critical Thinking: Final Report in Support of Air Combat Command [Review]," Integrity ISR (June 2020), 13.

⁵ DODIG-2019-032, *Evaluation of Combatant Command Intelligence Directorate Internal Communications Processes* (Washington, DC: DODIG, December 4, 2018), i, 11–12, <https://media.defense.gov/2018/Dec/11/2002071181/-1/-1/1/DODIG-2019-032.PDF>.

⁶ Sherrill L. Stramara, "Integrated Certification and Training for Intelligence Professionals," *MI Professional Bulletin* 41, no. 1 (January–March 2015), 21, <https://www.ikn>.

army.mil/apps/MIPBW/MIPB_Issues/MIPB-Jan_Mar15IKN.pdf.

⁷ James Kwoun, "The Limits of Intuition: Army Intelligence Should Embrace Analytic Tradecraft Standards," *War on the Rocks*, July 8, 2020, <https://warontherocks.com/2020/07/the-limits-of-intuition-army-intelligence-should-embrace-analytic-tradecraft-standards/>.

⁸ DODIG-2019-032, ii.

⁹ DODIG-2015-015.

¹⁰ DODIG-2019-032; Grunwald, Crouse, and Sullivan, "The State of Analysis and Critical Thinking," 15–16.

¹¹ "All-Source Analysis," Department of Defense Intelligence and Security Professional Certification, <https://dodcertpmo.defense.gov/CDASA/>.

¹² Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for a New American Security, January 2010), https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/AfghanIntel_Flynn_Jan2010_code507_voices.pdf?mtime=20160906080416&focal=none.

¹³ DODIG-2019-032, i.



Airman from 118th Intelligence, Surveillance, and Reconnaissance Group, Tennessee Air National Guard, examines images of tornado damage across Tennessee, March 4, 2020, at Berry Field Air National Guard Base, Nashville, Tennessee (U.S. Air National Guard/Anthony Agosti)



Secretary of State Antony J. Blinken delivers remarks at World AIDS Day event hosted by Business Council for International Understanding, in Washington, DC, December 2, 2022 (State Department/Ron Przysucha)

The Purpose and Impact of the U.S. Military HIV Research Program

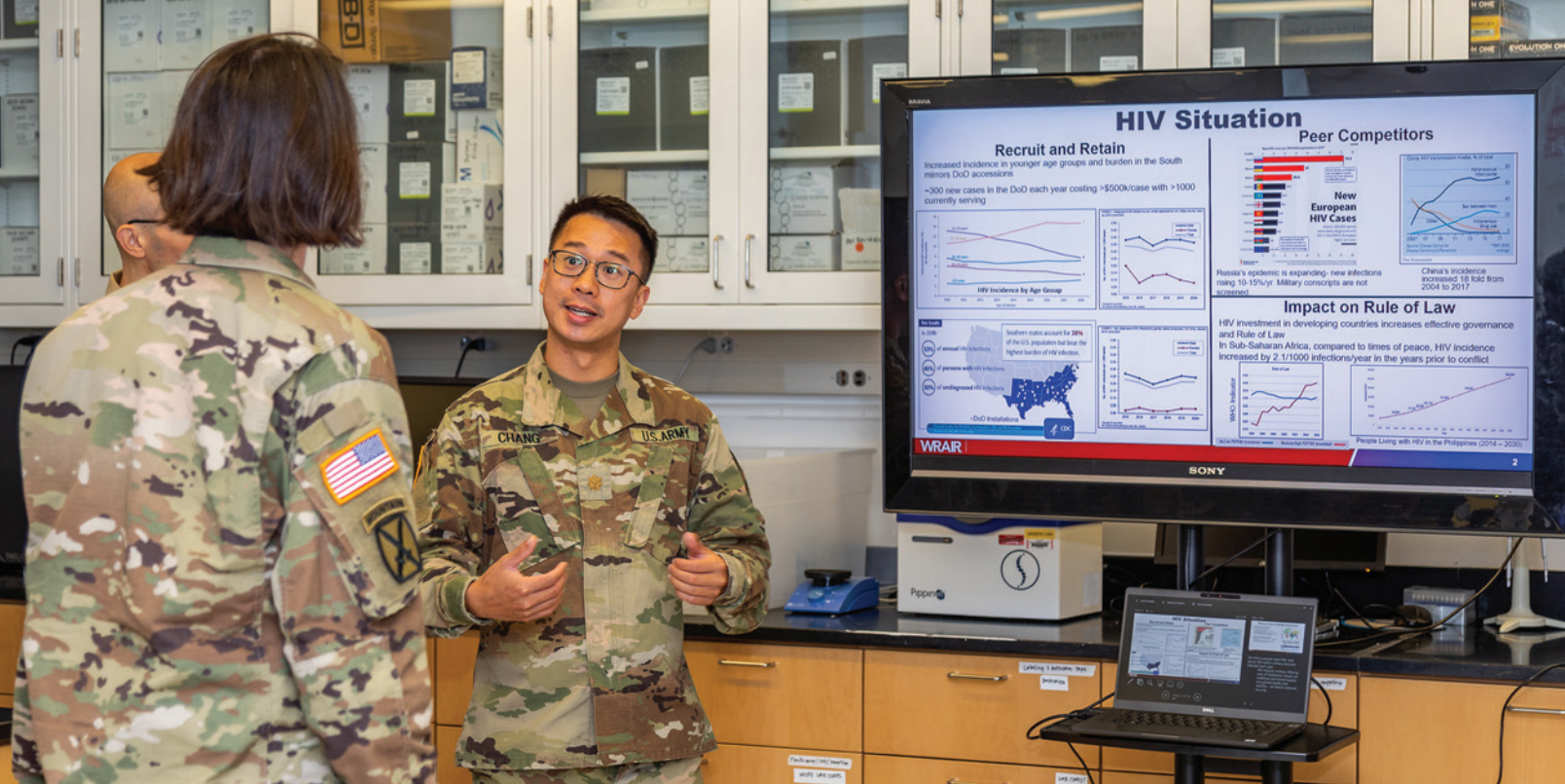
By Joseph S. Cavanaugh, Clinton K. Murray, David Chang, and Julie A. Ake

HIV, or the human immunodeficiency virus, has been acknowledged as a global epidemic since shortly after it was identified as the virus responsible for acquired immunodeficiency syndrome (AIDS) in the mid-1980s. The Joint United Nations Programme on HIV/AIDS estimates that almost 38 million people were living with HIV as of 2020, and more

than 36 million people have died from HIV-related illnesses since the beginning of the epidemic.¹ Evidence demonstrates that the prevalence of HIV is highly variable in militaries and tends to be higher than in comparable civilian populations in higher prevalence settings.² Most militaries screen for and exclude HIV-infected persons from conscription or enlisting, so detected

infections most likely occur after enlistment, suggesting that military personnel are often at substantially increased risk for acquiring and then possibly transmitting HIV.³ Researching and developing countermeasures for HIV have both operational and diplomatic benefits and are the founding objectives for the Military HIV Research Program (MHRP) at the Walter Reed Army Institute of Research (WRAIR). MHRP was established in 1986 to directly address the threats posed by HIV by conducting relevant research on prevention and treatment, evaluating the impact of HIV on U.S. Servicemembers, and developing strategies to

Captain Joseph S. Cavanaugh, MD, U.S. Public Health Service Commissioned Corps, is the Chief of International HIV Prevention and Treatment at the Walter Reed Army Institute of Research. Brigadier General Clinton K. Murray, USA, is Commanding General at the Brooke Army Medical Center. Major David Chang, USA, is the Chief of the Infectious Disease Service at Ft. Belvoir Community Hospital. Colonel Julie A. Ake, USA, is Director of the Military HIV Research Program at the Walter Reed Army Institute of Research.



Major David Chang and Captain Sean Cavanaugh brief Brigadier General Wendy L. Harter on the HIV Research Program at Walter Reed Army Institute of Research, June 29, 2021 (U.S. Army/Arlen Caplan)

protect military personnel—a mission that also addresses the global burden and consequences of HIV disease.

HIV is readily transmitted when infected body fluids break through the skin or mucosal membranes, as can happen with unprotected sexual contact or when infected needles or blood products are used. HIV spreads easily through sexual networks, especially those where barrier protection is not consistently used or commercial sex is practiced. Blood products should be universally screened for HIV, but this process takes time and is imperfect. Risks of breakthrough contamination are particularly elevated in high-volume, emergent transfusion environments, as seen during high-intensity conflict and expected during large-scale combat operations.

Untreated, HIV replicates in the human body to high viral loads, destroying the immune system as it does. High viral loads are associated with more rapid immune-system compromise and high infectiousness. The newest treatment regimens are highly effective at inhibiting viral replication and have turned HIV infection into a chronic, untransmissible condition associated with a normal or near-normal lifespan, much like other

chronic medical conditions such as diabetes or hypertension. The most widely used current treatment regimens are combination antiretroviral therapies taken as a daily pill. Successful management of HIV, however, requires diligent daily adherence, and lapses in treatment can result in progressive immune deficiency and onward transmission of the virus. Given the urgent need for rigorous adherence, and the costs associated with lifelong treatment, the most strategic approach is effective prevention for those at elevated risk of infection, including warfighters. This remains a top priority for global research efforts.

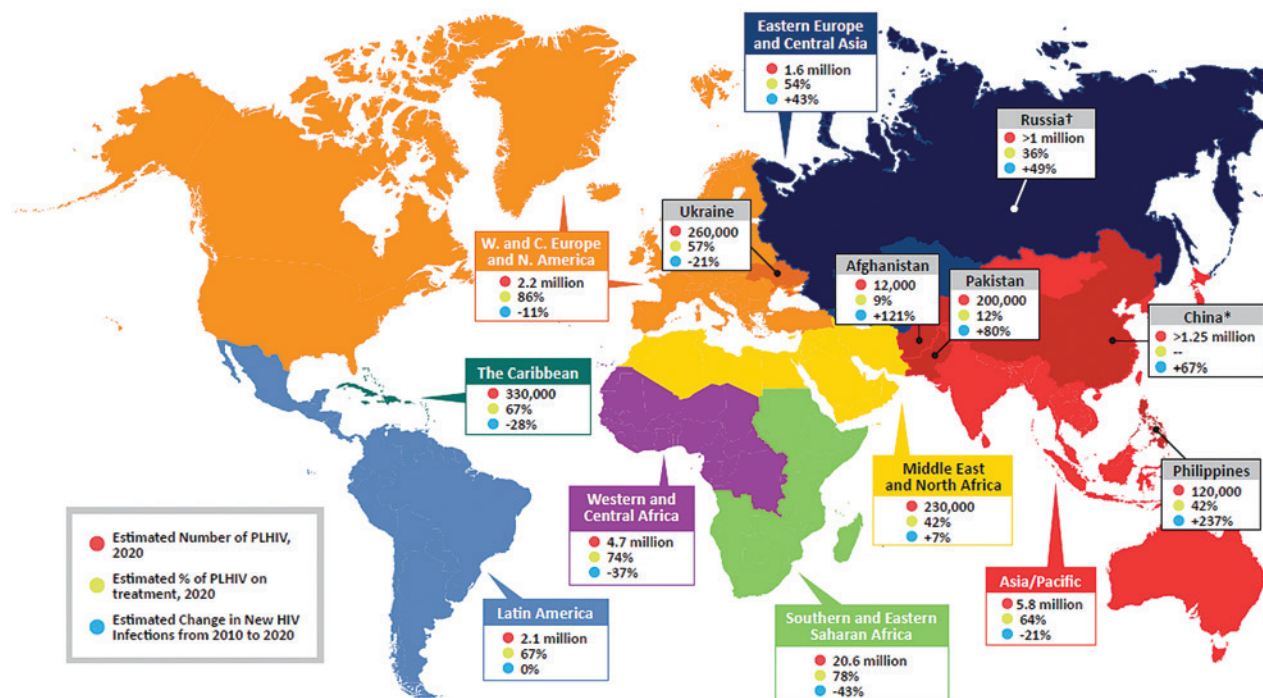
HIV is a threat to U.S. military interests for two principal reasons: the direct biomedical threat of, and the costs and consequences incurred by, infection to warfighters and the destabilizing effects that HIV may have on the sociopolitical systems of our strategic allies. MHRP has a multipronged strategy to counter these biomedical and sociopolitical threats posed by HIV.

Effective prevention of HIV infection is the cornerstone of the strategy, and MHRP has emerged as a leader in HIV vaccine research. Areas of research include both the development

of effective vaccines and “passive vaccination” approaches with monoclonal antibodies to directly neutralize HIV before infection is established. MHRP also conducts research in acute HIV infection to deepen understanding of the early events of infection. Intervening in acute infection allows for the evaluation of strategies to vastly simplify treatment or even present the possibility of a functional cure, or treatment that effectively suppresses viral replication and blocks immune decline and forward transmission without the requirement for ongoing therapy. In addition to these product development initiatives, MHRP collects and analyzes data on HIV epidemiology and threat patterns, using domestic and international observational studies of both military and civilian populations to identify opportunities to mitigate the risk of HIV and other sexually transmitted infections.

MHRP is also part of a broader Department of Defense (DOD) initiative to provide direct HIV-service delivery across the globe. DOD receives funding from the President’s Emergency Plan for AIDS Relief (PEPFAR) to support HIV services in the military health systems of countries hardest hit by the global HIV

Figure 1. HIV Prevalence and Incidence in Selected Countries



*Estimates for China are from modeled UNAIDS data in 2018

†Estimates for Russia are from UNAIDS data in 2017, some experts estimate 10–15% increase in HIV incidence each year with approximately 1.5M PLHIV in 2020

pandemic (military-to-military programs, supported principally by the DOD HIV/AIDS Prevention Program). Some of that funding goes to MHRP to provide an array of HIV services to civilian communities that participate in MHRP research (military-to-civilian programs). These activities represent a broad collaboration across the U.S. military and are a critical DOD tool to foster stability, promote goodwill, and enable strategic alliances and safer deployments.

HIV Threats to the Warfighter and Military Services

In the United States, HIV rates vary widely among groups, with the virus disproportionately affecting African Americans, Latinos, people who live in the American South, and, increasingly, those who are 25 to 34 years old—all groups highly represented in the U.S. military. These elevated infection rates have a negative impact on accessions; HIV remains a bar to enlistment because of restrictions on deployment and concerns about the ability

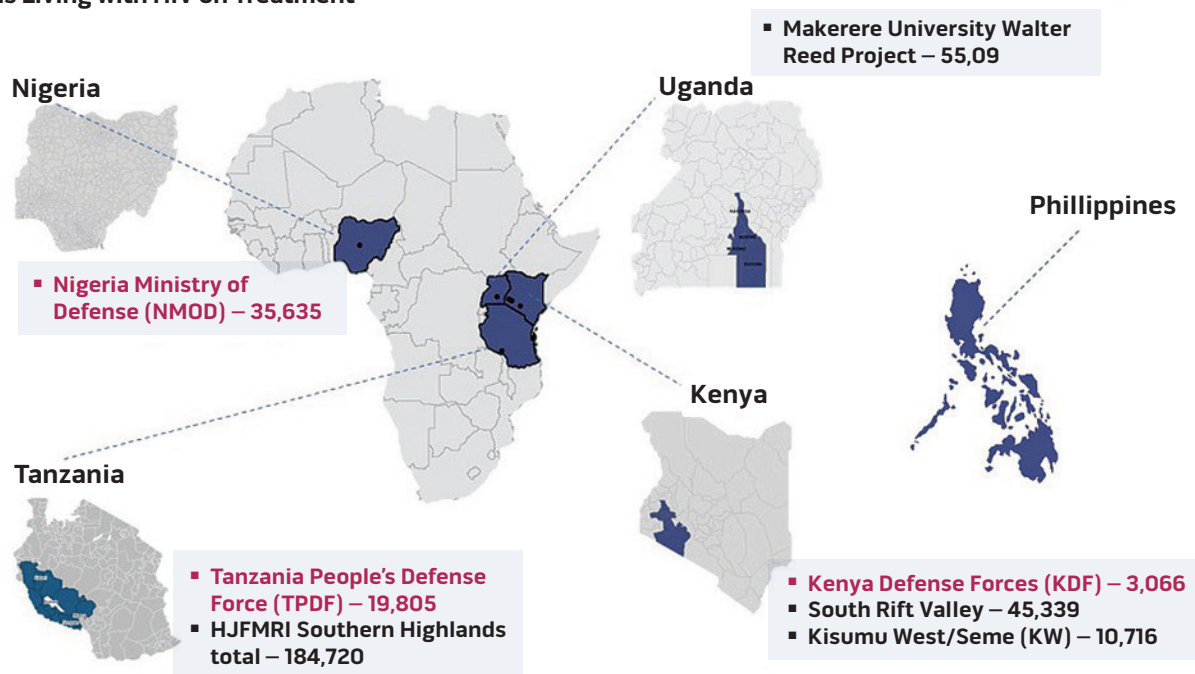
to maintain consistent treatment in battlefield conditions.

Similarly, the incidence of HIV varies widely across the globe, with particularly elevated rates of infection in many African and some Asian nations, and increasing incidence in Russia, Ukraine, China, Pakistan, the Philippines, Afghanistan, the Middle East, and North Africa, all of which are potential theaters of future military activity or strategic locations for U.S. military presence (figure 1). Of particular note, because of increasing potential for U.S. military presence, Ukraine has the second highest HIV incidence in Europe, behind only Russia, and HIV incidence in the Philippines has increased by an alarming 237 percent since 2010. In such countries, the increasing incidence of HIV and low coverage of treatment poses risks to U.S. Servicemembers through either sexual contact or exposure to blood, blood products, or sharps, which could occur on the battlefield or in forward surgical and medical units. The availability of sufficient and safe blood products during times of conflict is a growing

concern. A model run using the Medical Planners' Toolkit (and the Casualty Rate Estimation Tool) estimated that in a near-peer conflict with over 50,000 casualties in the first 4 days and 2,000 to 3,000 casualties per day after that, more than 70,000 units of red blood cells would be needed over the first 90 days.⁴ That need would rapidly deplete stocks of available blood products and overwhelm prescreened walking blood bank strategies and therefore pose risks to the supply and to effective treatment. If such a conflict were to happen in an area of rising HIV incidence, such as Russia, where an estimated 1.1 percent of the adult population is HIV-infected, breakthrough contamination to the blood supply employed in the emergent treatment of mass casualties would be likely.

There are approximately 350 new HIV infections among Active Servicemembers each year, almost all acquired through unprotected sexual activity, and it has been estimated that there are currently over 2,000 Active Servicemembers with HIV.⁵ These Servicemembers are typically not deployable given the potential

Figure 2. Countries Where MHRP Currently Implements HIV Programming, with Program Names and the Number of Persons Living with HIV on Treatment



for treatment interruption, which could compromise performance. At a lifetime treatment cost of over \$420,000 per HIV-infected Servicemember, HIV imposes a heavy financial burden on the U.S. Military Health System, a burden that could be alleviated by preventing infection and the long-term consequences of HIV disease.⁶ Preventing and treating HIV is not only a professional obligation for military clinicians, but it is also a tactical measure. Identifying and utilizing the most optimal biomedical tools yield a tactical advantage in medical readiness when facing adversaries that do not mitigate their own HIV threats.

Geopolitical Threats of HIV

In many ways, the more pervasive threat of HIV is not clinical but social and geopolitical. Like many infectious diseases, HIV is both a cause and a consequence of war and social unrest. In the 1990s and early 2000s, entire communities in certain countries were altered by the loss of their most active and productive members, which left them with unsupported orphans, a dwindling socioeconomic base, and increasing social disorder. Economic desperation and social disorder, either because of HIV itself or

as a consequence of civil unrest or war, contributed to forced and commercial sex, illicit drug trafficking, internal migration, and limited access to health care—thus creating environments even more conducive to the spread of HIV. The United Nations Security Council (UNSC) recognized HIV as an international security issue; it passed Resolution 1308 in July 2000, the first time that a health issue was acknowledged as a threat to peace and security. In June 2011, the UNSC passed Resolution 1983, recognizing the impact of HIV in conflict and postconflict environments.⁷

Health is a security imperative, central to the success of the combatant command missions. HIV threatens health security and if left unaddressed can undermine efforts to secure and stabilize volatile regions. As mentioned, military personnel may be at greater risk for acquiring and then transmitting HIV, and if those personnel do not have reliable access to affordable medications and quality health care, there is a real risk of amplifying transmission and compromising force readiness. In addition, in regions where U.S. forces serve alongside those of allies, high rates of infection can compromise the allied militaries, thus impeding U.S. strategic interests.

HIV Countermeasures

Prevention is the most cost-efficient and effective approach to the threats posed by HIV. There have been important advances in the use of medicines to reduce the risk of HIV infection, so-called pre-exposure prophylaxis (PrEP). Both daily and on-demand oral regimens and, more recently, investigational long-acting injectables have shown remarkable effectiveness at preventing infection in certain populations.⁸ MHRP has worked with Service clinical leadership to evaluate the use of PrEP in the military and identify military-specific issues. DOD is using findings from this research to identify gaps and barriers to care and to develop policy for its use; for example, currently available oral PrEP agents are now employed for HIV prevention in military treatment facilities but are not recommended as appropriate for use in deployed settings.

The most critical advance needed to protect against the threat of HIV is an effective vaccine. An effective vaccine would prevent the substantial morbidity and mortality associated with HIV without requiring adherence or exposure to medications, preserving force readiness at a cost substantially less than regular drug



Hospital Corpsman 1st Class Oliver Arceo draws blood for Sailor's annual HIV test at North Island Medical Clinic, Naval Air Station North Island, Coronado, California, January 7, 2017 (U.S. Navy/Marie A. Montez)

administration. MHRP is collaborating with government, academic, and industry partners to advance promising vaccine candidates to protect against global strains of the virus. To date, MHRP has conducted dozens of vaccine-related trials and conducted the only HIV vaccine study to show modest efficacy in reducing the risk of HIV infection. Although the higher level of efficacy needed to protect U.S. Servicemembers was not reached, MHRP's RV144 Thai trial provided proof of concept that an HIV vaccine is possible. MHRP continues to play a critical role in the international HIV vaccine field: among the eight most recent HIV vaccine efficacy trials (complete or ongoing), five included products that MHRP helped to develop. MHRP scientists are currently testing a novel adjuvant, called the Army Liposome Formulation, to improve immune responses to vaccines. MHRP participated in the early development of the Janssen mosaic vaccine candidate now being tested in two major multinational efficacy trials in a global partnership comprising the National Institutes of Health, Johnson and Johnson, major philanthropic organizations, and the U.S. military. Other planned studies will examine new vaccine products designed to optimize protection against HIV subtypes most common in the U.S. military as well as the effects of

rapid dose administration and product-sparing fractional dosing strategies.

Additional research is needed to protect the blood supply and wartime blood-product recipients from HIV infection. MHRP is researching the potential protective benefit of broadly neutralizing antibodies (bnAbs), which are long-lasting and may allow for injections as infrequently as every 3 or even 6 months. The use of bnAbs and post-exposure medicinal prophylaxis, potentially in combination with vaccine booster doses given at the time of transfusion, might mitigate infection risk for those receiving emergency blood products that were not adequately screened or that were collected from high-risk populations; such interventions require further investigation.

If prevention fails and infection occurs, provisions for lifelong therapy must be made. Effective management of HIV halts viral replication and stops forward transmission but is currently challenged by the need for daily pill adherence. Without regular adherence, HIV can replicate in the body at high levels, increasing the possibility of transmission and the likelihood that the virus develops genetic mutations that may cause drug resistance—both of which pose considerable threats to individual and public health. The need for fully reliable procurement and supply management is

therefore critical, but such management is difficult to guarantee, especially in prolonged conflict environments. Similar medicines with the same efficacy as daily pills can now be given as long-acting injectables monthly, allowing greater treatment flexibility and improving adherence.⁹ HIV might also be managed with infrequently dosed therapeutic bnAbs and/or vaccines, which MHRP is studying; if proven effective, such therapies could greatly reduce treatment burdens and allow for unrestricted deployment of HIV-infected individuals.

Countering Geopolitical Threats

Assisting other countries and foreign militaries with their own HIV responses provides an opportunity to strengthen U.S. alliances and conforms to the priorities described in the Interim National Security Strategic Guidance.¹⁰ Strategic health diplomacy is the idea that U.S. interests and foreign policy objectives can be advanced through investments in foreign health programs and the international health infrastructure. PEPFAR, established by a bipartisan congressional act in 2003, has been a cornerstone program for U.S. foreign health investment and one of the most successful strategic health diplomacy programs in U.S. history.

PEPFAR is the largest single global health program of the U.S. Government and the largest HIV prevention program in the world. PEPFAR funding, approximately \$6 billion to \$7 billion each year, is divided between the Global Fund to Fight AIDS, Tuberculosis, and Malaria and various U.S. agencies, including DOD, which direct the funding to implementing partners and ministries of health in more than 50 countries. The funding directly capacitates health systems with investments in medications; laboratory and clinical commodities; personnel and staffing; and critical surveillance, research, and evaluation efforts.

We owe a debt to the communities in which research of benefit to the U.S. military is conducted, and MHRP pays that debt by implementing HIV prevention and treatment programs in those communities, providing an ethical framework for the clinical research it conducts. This programming also builds strong relationships with host communities, including local military and civilian partners, and establishes a foundation for security cooperation in strategic locations.

MHRP channels its PEPFAR funding into eight implementing mechanisms in five countries: three in Kenya, two in Tanzania, and one each in Nigeria, Uganda, and the Philippines. Four of these are military-to-military partnerships, and four are military-to-civilian programs (figure 2).

The military-to-military programs are cornerstone elements of security cooperation with partner militaries, and the military-to-civilian programs are quite visible in their respective communities and have helped cultivate enduring goodwill among DOD, the militaries, the ministries of health, and the civilian communities in the countries where PEPFAR operates. Long-term positive and productive relationships developed through partnering for HIV service delivery provide a consistently good news story for bilateral relationships and make possible other important conversations among the militaries.

A key strategic component is the substantial investment in case-finding and sufficient laboratory capacity, including

automated molecular machines that can detect multiple diseases using various specimens. These instruments can be strategically placed near the points of care across each PEPFAR-supported country to maximize access and accelerate timeliness of results. The diagnostic platforms are crucial for HIV diagnosis and service delivery but can be utilized for other disease detection, most recently COVID-19. This will enable countries to establish sensitive surveillance to emerging infectious threats and mount appropriate and timely public health responses.

Through direct investment in clinical service delivery, PEPFAR has made possible efficient and highly effective community-level HIV treatment and prevention and has laid the groundwork for comprehensive healthcare systems. The clinical infrastructure is currently being used to diagnose, treat, and prevent other infectious diseases in the broader population and can be leveraged to support noncommunicable diseases as well. The net result has been a radical improvement in the health of the communities that were previously ravaged by HIV, with an estimated 20 million lives saved by PEPFAR-supported efforts.¹¹ The effectiveness of these investments has brought stability to entire regions and has helped promote good governance across the many nations that PEPFAR supports.

The investments in HIV prevention and treatment have clear benefits to U.S. foreign policy and military interests. By promoting force health protection among U.S. Servicemembers and members of allied military forces, we are maintaining a competitive advantage and helping stabilize communities around the world. The development of an effective vaccine for HIV will be a truly historic accomplishment that could save millions of lives, provide full protection for Servicemembers, and allow great gains in strategic health diplomacy. The U.S. military's visible programmatic investments and research successes directly support U.S. combatant commands and have fostered profound good will and helped strengthen strategic alliances across the globe. JFQ

Notes

¹ "Global HIV & AIDS Statistics—Fact Sheet," Joint United Nations Programme on HIV/AIDS, 2023, <https://www.unaids.org/en/resources/fact-sheet>.

² Jennifer Lloyd et al., "Systematic Review and Meta-Analysis of HIV Prevalence Among Men in Militaries in Low Income and Middle Income Countries," *Sexually Transmitted Infections* 90, no. 5 (August 2014), 382–387.

³ Deborah Bix, Richard Shaffer, and Marc Bulterys, "Foreword: HIV in Military Populations," *Current HIV Research* 15, no. 2 (2017), 76.

⁴ Edwin D'Souza et al., *Forecasting Wounded-in-Action Casualty Rates for Ground Combat Operations* (San Diego, CA: Naval Health Research Center, August 2019), <https://apps.dtic.mil/sti/pdfs/AD1105971.pdf>.

⁵ Bryce H.P. Mendez, *HIV/AIDS in the Military*, IF11238 (Washington, DC: Congressional Research Service, May 31, 2019), <https://sgp.fas.org/crs/natsec/IF11238.pdf>; Erik Larson, "The Military Is Waging War on HIV-Positive Soldiers," *Bloomberg*, September 22, 2020, <https://www.bloomberg.com/news/features/2020-09-22/u-s-armed-forces-can-prevent-hiv-positive-recruits-from-enlisting>.

⁶ Adrienna Bingham et al., "Estimated Lifetime HIV-Related Medical Costs in the United States," *Sexually Transmitted Diseases* 48, no. 4 (April 2021), 299–304, https://journals.lww.com/stdjournal/Fulltext/2021/04000/Estimated_Lifetime_HIV_Related_Medical_Costs_in_15.aspx.

⁷ "Unanimously Adopting 1983 (2011), Security Council Encourages Inclusion of HIV Prevention, Treatment, Care, Support in Implementing Peacekeeping Mandates," SC/10272, United Nations, June 7, 2011, <https://un.org/press/en/2011/sc10272.doc.htm>.

⁸ "PrEP (Pre-Exposure Prophylaxis)," Centers for Disease Control and Prevention, June 3, 2022, <https://www.cdc.gov/hiv/basics/prep.html>; "Trial Results Reveal that Long-Acting Injectable Cabotegravir as PrEP Is Highly Effective in Preventing HIV Acquisition in Women," World Health Organization, November 9, 2020, <https://www.who.int/news/item/09-11-2020-trial-results-reveal-that-long-acting-injectable-cabotegravir-as-prep-is-highly-effective-in-preventing-hiv-acquisition-in-women>.

⁹ "FDA Approves Cabenuva and Vocabria for the Treatment of HIV-1 Infection," U.S. Food and Drug Administration, January 27, 2021, <https://www.fda.gov/drugs/human-immunodeficiency-virus-hiv/fda-approves-cabenuva-and-vocabria-treatment-hiv-1-infection>.

¹⁰ *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>.

Green Berets with 2nd Battalion, 1st Special Forces Group (Airborne), and Explosive Ordnance Disposal Specialists with 25th Infantry Division conduct clearing procedures while evacuating simulated casualty during Joint Pacific Multinational Readiness Center rotation 23-01 training exercise on Schofield Barracks, Hawaii, November 7, 2022 (U.S. Army/Ryan Hohman)



Special Operations Forces Institution-Building

From Strategic Approach to Security Force Assistance

By Kevin D. Stringer

The Ukrainian Special Operations Command (UKRSOCOM) and its subordinate tactical units have emerged as significant contribu-

tors to the defense of Ukraine in the face of ongoing Russian aggression. Conducting a full range of both conventional and special operations

missions—including mobile defense, guerrilla operations, direct action, and support to resistance in occupied areas—UKRSOCOM displays the qualities of a rapidly maturing special operations organization currently being tested in the crucible of combat. A contributing element to the development of UKRSOCOM as an institution was

Colonel Kevin D. Stringer, USA (Ret.), Ph.D., is the Chair of Education for the U.S. Irregular Warfare Center. He is an affiliated Faculty Member at the General Jonas Žemaitis Military Academy of Lithuania, in Vilnius.

an experimental U.S. Special Operations Command Europe (SOCEUR) advisory approach, based on an earlier initiative with Belgium, that aimed to establish a framework for developing and sustaining special operations forces (SOF)'s institutional capabilities at the national level.

As background, U.S. SOF invested years in advising and assisting European partners to build and deploy special operations tactical units of excellence to campaigns in Afghanistan, Iraq, and Syria, as well as counterterrorism actions globally. Unfortunately, while U.S. SOF concentrated on advising at the tactical level, they ignored the institutional level. Gradually, many European states realized they possessed an insufficient strategic SOF institutional framework for sustaining forces and organizing national and coalition operations in an emerging near-peer threat environment. This situation reconfirmed a recurring problem within broader U.S. security force assistance (SFA)—a tendency to build a force without first establishing the necessary institutional framework.¹ Maintaining SOF capability requires establishing the defense institutional systems that can contribute to SOF development. By 2014, certain European policymakers recognized the requirement for strategic-level SOF structures to address a deteriorating European security environment and to better manage and employ scarce SOF human and material resources.² Beginning in 2016, SOCEUR, in collaboration with North Atlantic Treaty Organization (NATO) Special Operations Headquarters (NSHQ), pioneered a SOF institution-building (SOFIB) advisory approach, nested within the broader U.S. security cooperation (SC) concept, to support specific NATO Allies and select partners in their development of special operations command (SOCOM)-like structures intended to unify various national units while providing SOF-specific institutional functions for a more effective and sustainable force. Given the inherent joint nature of SOF, these SOFIB insights offer the joint forces recommendations on SFA activities in the future.

This article highlights the SOFIB approach and its nesting within the U.S. SC and SFA framework. It then shows how SOFIB reconceptualizes SFA from its heavy tactical application, as seen in Afghanistan, Somalia, and Syria, and shifts efforts to national- and institutional-level defense assistance for capable European allies and partners. It then illustrates the application of SOFIB through the representative but differing cases of Belgium and Ukraine, while providing an overview of the supporting SOCEUR and, in the case of Ukraine, NSHQ strategic advisory efforts, using SOFIB objectives as a framework of analysis. The article then provides overall joint lessons learned concerning SOF transformation at the national level that can inform SFA best practices for the future.

SC, SFA, Foreign Internal Defense, and SOFIB

SOFIB is nested within the overall U.S. SC and SFA framework but differs from SC and SFA generic activities with its concentration on SOF as well as its advising focus at the national and institutional levels. SOFIB also differs from foreign internal defense (FID) because of its stronger accent on peacetime engagement at the institutional level to prepare for both internal and external threats. SC is a broad range of programs and activities that the U.S. Department of Defense (DOD) executes on behalf of the U.S. Department of State as well as “all [DOD] interactions, programs, and activities with foreign security forces (FSF) and their institutions.”³ It could thus be any advisory program or mission between the United States and another country. The United States pursues SC for a number of reasons, with one being to support the institutional development of foreign security organizations.⁴ This last motive is actually SFA, defined as “the set of DOD activities that contribute to unified action by the [U.S. Government] to support the development of capacity and capabilities of FSF and their supporting institutions.”⁵ In contrast, FID, defined as the “participation by civilian agencies and military forces of a govern-

ment or international organizations in any of the programs and activities undertaken by a host nation government to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security,” is traditionally a SOF mission with a strong focus on internal threats. SOFIB falls more readily within the SFA space rather than that of FID, given its stronger emphasis on peacetime engagement at the institutional level to prepare for both internal and external threats.⁶

Traditional SFA has not been without problems.⁷ Most approaches seem to concentrate too much on the tactical level, to include training and equipping, as opposed to more valuable SFA programs, which address “higher-order questions of mission, organizational structure, and personnel.”⁸ Major SFA failures in Iraq and Afghanistan have led to serious questions about its efficacy as an instrument of U.S. national security policy.⁹ In these two countries, the United States invested billions of dollars as well as the human resources to support two decades of training and advising the security forces—only to watch them collapse in the face of so-called Islamic State or Taliban offensives.¹⁰ On a spectrum of partner development, traditional SFA seems to best describe U.S. activities with weak states such as Afghanistan and Somalia, whereas security “defense cooperation” better characterizes advising capable allies and partners to improve their combined operations.¹¹

One example of this delineation can be found in Ukraine. Although Russian actions are dangerous for Ukraine in the current war, Ukraine is not a weak state, and its military has capabilities; hence, U.S. assistance aims to improve national warfighting competencies often “through . . . ideational assistance.”¹² This latter emphasis characterizes the SOFIB methodology for peer or proficient SOF partners. The SOFIB approach aligns with the view that at the strategic level, U.S. advising objectives may achieve the greatest returns by emphasizing the development of more sophisticated headquarters functions and staff efficiencies, which enable upper-tier partner



Belgian special forces sniper team identifies targets 2,000 meters away, September 11, 2018, during International Special Training Centre High-Angle/Urban Course, at Hochfilzen Training Area, Austria (U.S. Army/Benjamin Haulenbeek)



Belgian special forces sniper teams fire on long-range targets from elevated shooting range during International Special Training Centre High-Angle/Urban Course, at Hochfilzen Training Area, Austria, September 30, 2020 (U.S. Army/Patrik Orcutt)

interoperability.¹³ Furthermore, with capable allies and partners, the accent is on liaison, consulting, and advisory activities as opposed to training, exercises, and support. The result of such a strategic- and national-level advisory effort is the aspirational pinnacle of security force effectiveness—combined, joint, and inter-agency integration and effectiveness.¹⁴

SOFIB Requests for Support and SOFIB Objectives

In 2016, SOCEUR received requests from several European countries for assistance with establishing SOF command structures and organizations

at the national level appropriate for their state security missions and military cultures. Both the changing European security environment and NATO pressure contributed to the need for SOF transformation and reform. For the environment, the rise of Russia as an adversary and Islamic terrorist attacks in Europe catalyzed national military discussions about the role and organization of SOF. Additionally, NATO encouraged member states to make structural reforms to their SOF beginning in 2013. The primary aim was to address SOF shortfalls, particularly in SOF command and control capabilities.¹⁵

In creating these strategic organizations, the European SOF counterparts aimed to achieve a mix of four general SOFIB objectives:

- SOF autonomy, defined as the national SOF institutions' achievement of a greater degree of independence from the respective military services. This goal endeavored to elevate an integrated SOF organization within a national defense hierarchy to increase SOF independence and reduce subordination to the conventional land, sea, and air services. The generic issue is that without a unique



SOF command or proponent, conventional military services are often uninterested in SOF as a joint entity, with the resultant underemployment or misuse of SOF capabilities.

- Joint and interagency SOF integration, defined as the establishment of unity of command for joint SOF elements as well as the creation of greater connections to other relevant national agencies. This aspiration intended to consolidate often distributed SOF joint functions under one command while structurally enhancing interagency collaboration through the elevation of permanent

SOF representation and expertise to the general or joint staff level.

- SOF operational command and control (C2) capabilities, defined as the creation of a SOF national-level headquarters element with a core SOF organization and staff. The goal was to establish a C2 capability for NATO, regional, or coalition constructs while taking control and oversight of SOF readiness, capability development, and operational employment.
- SOF service-like competencies, defined as man, train, and equip functions, in order to better manage SOF recruitment, improve retention, own budget resources, and control SOF-specific procurement.¹⁶

Given the above objectives, and the fact that this type of strategic advisory effort was neither a standard SOCEUR nor a standard U.S. Special Operations Command mission, SOCEUR reorganized an existing staff division in 2016 to support a group of prioritized countries on their journeys to establish national SOCOM-like entities. Belgium and Ukraine serve as illustrative vignettes of the SOFIB application. To note, the respective U.S. country team senior defense officer (SDO) and office of defense cooperation (ODC) facilitated the SOFIB requests from both Belgium and Ukraine but were not directly involved in the advisory process.

Belgian Special Operations Command Initiative

In 2016, the Belgian Ministry of Defense published its *Strategic Vision for Defence* through 2030. This national security document led to the creation of the Belgian SOCOM and initiated the start of a larger SOF change project. Prior to the publication of this strategic guidance, Belgian SOF capabilities were centered on a single tactical formation that was increasingly underresourced for an expanding joint and interagency mission set. Key considerations for this transformation included the increasing relevance of irregular warfare, the use of Belgian SOF for homeland security and counterterrorism operations, the require-

ment to protect Belgian citizens abroad, and the rise of Russian aggression on the Eastern European periphery.¹⁷ The *Strategic Vision* mandated a transformation of Belgian SOF to include:

- establishment of a SOF command to better manage special operations
- investments in a Tier 1 special forces group to include a personnel expansion of its core elements
- conversion of the two airborne para-commando battalions into Ranger-like units with specialized enablers—air assets, counter-improvised explosive device experts, and military working dog teams
- acquisition of several short takeoff and landing (STOL) aircraft specific to SOF
- participation of Belgian SOF in a composite special operations component command (C-SOCC), together with the Netherlands and Denmark, to meet NATO SOF operational C2 requirements.¹⁸

A critical element of this change was the creation of a to-be-defined SOCOM to oversee the command and development of Belgian SOF. This step would also provide a national-level mechanism for better connecting to Belgian intelligence, law enforcement, and diplomatic agencies.

The Belgian SOF project team requested SOCEUR advisory support to discuss the overall SOF transformation and the specifics of the Belgian Special Operations Command (BELSOCOM) requirement. The U.S. national interest in supporting this initiative was the opportunity to greatly enhance the SOF capabilities of an important NATO Ally for future combined, coalition, or Alliance operations, as well as potential SOF burden-sharing in regions of mutual importance. A unique aspect of this and other SOFIB advisory efforts was its strategic and iterative, rather than instructional and tactical, nature, given the peer-to-peer SOF relationship. Belgian SOF possess high levels of expertise and capability; hence the advising relationship could be likened to that of collaborative partners in a consulting or executive

coaching arrangement. The initial workshop focused on the topics of project setup and management, to include governance. An early recommendation was the need to structure the steering committee with general officer-level sponsorship and appropriate interagency representation to ensure a successful outcome. Through the exchange, both teams agreed that a Belgian-specific doctrine, organization, training, materiel, leadership (and education), personnel, and facilities (DOTMLPF) framework would serve as a good structure for this complex transformation.

After analysis and acknowledgment of potential Belgian organizational and political resistance, key U.S. design recommendations were to establish a unified joint SOF command and staff on par with the land and air component commands, directed by a one- or two-star general officer. Interestingly, this U.S. proposal mirrored that of a Belgian think tank brief, which advocated the creation of a flag officer-led SOCOM, light enough to lead national special operations activities yet robust enough for the C-SOCC contribution.¹⁹ If this step was too great, the U.S.-recommended interim stage was the stand-up of a SOF directorate, subordinated to the chief of defense, to facilitate the transition. A secondary U.S. recommendation was for the definition of what a Belgian para-commando unit should accomplish for SOF tasks, and the identification of the capability gaps within its existing mission sets, organization, training, and equipment. The U.S. advisors cautioned against simply copying either the U.S. Ranger Regiment or the British Special Forces Support Group model, considering them inappropriate for Belgian needs. Additionally, both the Belgian and U.S. teams agreed to conduct further analysis on the integration of SOF air assets into the new structure. For the latter point, the Belgian *Strategic Vision* authorized a specialized SOF aviation capability consisting of four small STOL aircraft, primarily for SOF insertions and extractions in austere environments.²⁰ Given that these assets were totally new in the force structure, would require some level of joint integration with the

conventional air force, and would introduce greater joint complexity for even a very capable peer, the SOCEUR team recommended a separate and more detailed follow-up meeting with a U.S. SOF air advisory team.

Belgian Special Operations Command Outcomes

Ultimately, Belgian defense leadership accepted the majority of the Belgian project team's transformation recommendations, and the outcomes of this case provided instructive SOFIB lessons for U.S. SOF. The selected Belgian generic model of SOF organization comprises a SOCOM integrated in the general staff, with the SOF tactical units placed under a regimental (brigade)-level headquarters and maintained under service jurisdiction for readiness purposes.

BELSOCOM emerged as a small, embedded special operations directorate within the general staff, led by a colonel (foreseen to be a brigadier general). BELSOCOM is the SOF advisor for the chief of defense and the larger defense staff. It serves as the central hub for all SOF matters and is responsible for aligning the national SOF structure to defense requirements. BELSOCOM is the primary point of contact for all joint, combined, and interagency cooperation. BELSOCOM also conducts strategic foresight activities and contributes to the planning and direction of all special operations.²¹ Explicitly, BELSOCOM is "designed to facilitate cross ministry cooperation and ensures Ministry of Defense and General Staff policies, programs, budgets, strategies, and regulations account for, and enable the development, sustainment, and employment of, Belgian Special Operation Forces."²² BELSOCOM assists the newly created Special Operations Regiment in fields such as the strategic planning of SOF capacity (included in the NATO defense-planning process), planning the future employment of SOF, and the procurement of SOF-specific items. The then Belgian minister of defense, Steven Vandeput, reiterated that BELSOCOM is the crucial integrating element in the new SOF regiment's environment. He stated:

Together with the creation process of the Special Operations Regiment, a Special Operations Command . . . was set up in mid-2017. Although the SO units don't directly come under the SOCOM, the latter can be considered as the Belgian center for expertise for special operations. Because of its place in the defense structure, SOCOM is the point of contact for international and interdepartmental cooperation concerning special operations. SOCOM is also in charge of drafting the Composite Special Operations Component Command project where Belgium, with the Netherlands and Denmark, is developing a deployable SOF HQ that can be made available to NATO.²³

At the tactical and operational levels, the SOF organization remained under the auspices of the Belgian Land Component Command. The existing conventional Light Brigade, under the leadership of a colonel, was rebranded and converted to the Special Operations Regiment, composed of the Special Forces Group, the 2nd Commando Battalion, the 3rd Parachute Battalion, the battalion-level 6th Communication and Information Systems Group, and related training centers. Much more than just a name change, this alteration initiated a series of changes in multiple dimensions. The Special Operations Regiment now commands all special operations land forces and is entrusted with their permanent training, instruction, and personnel management.²⁴

For NATO purposes, BELSOCOM led the creation of the C-SOCC with its Dutch and Danish counterparts. The genesis for the C-SOCC concept occurred in the fall of 2013, when during a NATO SOF commanders' conference in Norway, the delegates of four nations were invited to a sidebar meeting with an NSHQ representative. At the time, NSHQ was looking for ways to increase NATO SOF C2 capacities. The idea was to generate more special operations component commands (SOCCs) to support NATO's operations.²⁵ A SOCC is a headquarters formation of 70 to 150 personnel who provide an organic, rapidly deployable C2 node for NATO contingencies.



Ukrainian President Volodymyr Zelensky presents state medals to Ukrainian Special Operations Forces during ceremony, July 29, 2022, in Odesa, Ukraine (Ukrainian Presidential Press Office)

The initial objective was to prepare a C-SOCC for a NATO Response Force (NRF) commitment. To succeed, it needed high-level ministry of defense support, and in 2017, the defense ministries of Belgium, the Netherlands, and Denmark signed a letter of intent, formalized in 2018 with a memorandum of understanding, that facilitated the endeavor. According to the Special Operations Regiment's commander:

The project team had to overcome many obstacles to include the identification of common procedures, establishment of ways to share classified information, and the creation of[a] multi-year training schedule

to build the capacity. . . . With regard to staffing, positions had to be distributed in a balanced manner between the three nations, with the key positions rotating according [to] a fixed schedule.²⁶

The new BELSOCOM construct was instrumental in allowing the Belgian defense ministry to successfully execute this initiative. Eventually, after having conducted multiple exercises under the scrutiny of NSHQ, the C-SOCC was declared fully operational in 2020; it became the NRF SOCC in 2021.²⁷ Thereafter, it remains a core SOF C2 node for future Alliance or coalition requirements.

In light of the SOFIB objectives, the BELSOCOM case demonstrates the challenges of SOF organizational transformation. For SOF autonomy, Belgian SOF (BELSOF) did not become their own service but gained a higher degree of self-sufficiency under the Belgian Land Component. For integration, the creation of BELSOCOM as a special operations directorate offered a central node for interagency interactions. This decision follows best practice in that SOF perform exceptionally well when supporting a comprehensive interagency effort.²⁸ BELSOCOM also provides the project core for SOF operational C2 capabilities in the form of the trinational C-SOCC.



Belgian paratrooper assigned to Special Forces Group, Special Operations Regiment, performs freefall jump under supervision of jumpmasters assigned to CE Para training center, on Chièvres Air Base, Belgium, April 19, 2022 (U.S. Army/Pierre-Etienne Courtejoie)

BELSOCOM's placement within the general staff serves as an initial step to its development of service-like functions. This important implementation step created a double challenge. On the one hand, the SOCOM had to find its place within the general staff, and on the other hand, the relationship between the SOCOM and the services had to be clearly and iteratively defined. In essence, although not all SOFIB objectives were fully met, the interim result produced a more strategic and capable SOF construct for Belgian national security, as well as enhanced interoperability

and collaboration with its U.S., European Union, and NATO partners.

In this case study, U.S. SOFIB, as a more refined and strategic form of SFA, contributed to this outcome with U.S. advisors serving as “sparring partners” and “consultants” for a peer ally. With this enterprise effort, the overall BELSOF capability is poised to provide policymakers with an expanded range of scalable, immediately available, and increasingly sophisticated joint options that can be employed as an initial response to a variety of crises or as a complement to

other national, international, or inter-departmental capabilities. BELSOF is committed to continually challenging and reinventing itself to remain effective and relevant—especially in the new security environment, seemingly subjected once again to Great Power competition.²⁹

Ukrainian Special Operations Command Endeavor

In contrast to Belgian SOF's longstanding membership and efficacy within NATO and its high level of interoperability with Allies, particularly

the United States, Ukrainian SOF had a very different starting point for its institution-building endeavors. As an offspring of the Soviet Union's special forces (Spetsnaz), Ukrainian SOF inherited a Soviet-style hierarchy and a culture and mindset that were not conducive to integration with Western special forces units. With U.S. assistance, Ukraine undertook efforts to modernize its SOF in the early 2000s, but by 2009 the project was halted due to a lack of Ukrainian political support. As early as 2008, the Ukrainian general staff and ministry of defense had attempted to develop a consolidated and independent SOF service within the Ukrainian armed forces, but the government rejected this initiative. From 2008 to 2015, a special operations directorate operated within the general staff as a coordination and advising element, with special forces dispersed across different services and branches of the Ukrainian armed forces and mostly misused as "elite" infantry.³⁰

Catalyzed by Russian aggression in Crimea and the Donbas in 2014, Ukrainian political leadership initiated several NATO-supported defense and security reforms, which included specific mandates to transform its SOF. In 2015, the general staff and ministry of defense developed and signed a concept for the formation and development of the SOF and simultaneously established UKRSOCOM.³¹ Two enduring institution-specific challenges during this period were the dispersion of SOF capabilities and responsibilities across a number of military, intelligence, and internal security organizations, and the residue of the earlier Soviet-style culture.

In 2016, Ukraine's parliament passed a law creating the Special Operations Forces of the Armed Forces of Ukraine (UKRSOF) as a separate and independent service within the armed forces, with the appropriate consolidation of existing special forces units under one command.³² This decision allowed the genesis of a U.S. SOFIB advisory initiative tasked with assisting with the development of UKRSOCOM and the transformation of its subordinate units

into NATO-compatible forces. Because this transformation is ongoing as of this article's publication, as well as affected by the continuing war with Russia, the next sections cover only the 2017–2019 period.

In 2017, upon mutual agreement, UKRSOCOM requested an initial SOCEUR advisory team to conduct a SOFIB scoping workshop. This initiative aligned with U.S. national interests to support Ukraine as a developing European partner as well as to counter Russian aggression on Ukraine's eastern front. Although the valuable SOFIB experiences from Belgium and another NATO country aided preparation for this initial engagement, there were a number of issues that emerged in hindsight. In general, this advisory mission was much more complex than the BELSOCOM collaboration because of both the Ukrainian starting point and the U.S. and Ukrainian shortcomings in the advisory relationship. Additionally, there were notable differences between working with a longtime, interoperable NATO Ally versus an emerging, non-Alliance partner. U.S. mission analysis determined that the initial advising stage would concentrate heavily on UKRSOF force design, force generation, and SC requirements. Unknown to the well-meaning U.S. advisors, Lithuanian SOF had already been in place since 2014 in an institutional advisory role and were dual-hatted to represent the NSHQ in Ukraine in 2015. Lithuania had assisted UKRSOCOM with the development of a SOF development plan circa 2015–2016, but this proposal was totally overlooked in the U.S. SOFIB effort.³³ Aspects of the Lithuanian proposal eventually seeped into the overall plan, but this oversight cost valuable time and understanding.

For force design, the collaborative session, conducted with Lithuanian SOF participation, produced a high-level concept of five components. First, it proposed new staff configurations and education at the UKRSOCOM level. Second, it recommended restructured units and staffs at the three primary subordinate SOF regiments—the 3rd, 8th, and 73rd. Third, it articulated a process to link special forces qualification at

the Ukrainian 142nd Training Center to regimental manning. Fourth, it urged that force generation through a revised qualification course become an essential element in staffing the regiments and UKRSOCOM with SOF-qualified personnel. Finally, the SOFIB sessions identified the necessity for a heavy SC component, in both education and equipment, for transforming UKRSOCOM. This SC element was significant for the SOFIB effort for both political and interoperability reasons. Geopolitically, the provision of U.S. SOF equipment and training was intended to wean UKRSOCOM from its Russian legacy, while simultaneously increasing interoperability with both U.S. and NATO forces.

For the American advisors, knowledge in special forces organizational design within a NATO context, special forces qualification program management, and SC became essential to providing the right guidance and advice in this initial SOFIB phase. Unfortunately, on the first point, SOCEUR advisors were often unfamiliar with NATO doctrine and standards, resulting in Ukrainian SOF's receiving force design inputs that were compatible to, but not fully in line with, NATO doctrine and standards. This gap required adjustments in later years to meet NATO certification standards.

For the Ukrainian special forces qualification course, the SOFIB design did not consider several critical elements. Most significantly, the personnel intake, output, and retention calculations were off, resulting in a manning plan that did not fully achieve its objectives. Additionally, a 6-month qualification course, followed by additional advanced skills training, proved unsustainable when juxtaposed with Ukrainian SOF deployment requirements against the Russian-supported separatist regions. Finally, the program did not include an instructor qualification component. Thus, when trainers attrited, the United States was left with the responsibility of training the next set of instructors.

Finally, security assistance was based on U.S.-generated tables of organization and equipment, which were inaccurate.

Equipment deliveries for Ukrainian SOF units were not timed to coincide with development priorities, nor was the United States aware of the Ukrainian requirement to certify equipment for use. As a result of this requirement, SOF equipment (such as boats) sat idle for extended periods of time (over a year) while awaiting certification.

The main partner challenges were threefold. First, UKRSOCOM's lack of English-language skills at the senior level made the use of qualified interpreters essential to overcome the communication barrier. This condition introduced a cumbersome element in all interactions; it expanded the time required for discussions and placed emphasis on interpreter quality, given the institutional level of the discussions. Second, the UKRSOCOM point of departure for transformation created a much longer time horizon for institutional change. Unlike Belgium, with its highly proficient and established NATO SOF force, Ukraine was just at the beginning of its SOF institutional journey. This situation meant that SOCEUR SOFIB efforts would require strategic patience through several U.S. command cycles and over consecutive fiscal years. Third, UKRSOCOM lacked "jointness." A SOF air component did not exist, and the maritime component had been decimated by the Crimean invasion with the loss of its basing, equipment, and personnel. These circumstances would necessitate a multiyear SC package for reviving, equipping, and training these joint elements. On the U.S. advisory side, one main cultural SFA bias needed to be overcome. The Afghan and Iraqi SFA experiences had reinforced the tendency to provide U.S. solutions and models that were wholly inappropriate for partner forces. This troubling trend leads to suboptimal outcomes, especially at the institutional level, where a partner does not have the culture, staff capacity, or resource capabilities to sustain a U.S.-inspired force model. As U.S. SOFIB advisors rotated on the UKRSOCOM initiative, this cultural issue was closely monitored.

As the discussions progressed, a further significant issue to address was the need to nest SOCEUR SOFIB efforts

within a broader NATO framework and context to avoid duplication of effort. In response to Russian aggression, NATO had reinvigorated its support to Ukrainian defense and security reforms, which the Alliance defined practically through the partnership planning and review process (PARP) and more recently established comprehensive assistance package (CAP) for Ukraine.³⁴ Operating within the frameworks of the PARP and CAP, NSHQ rendered advice and assistance to Ukrainian SOF development, guided by Ukraine's initially stated aim of achieving full NATO interoperability by 2020. Alongside NSHQ's organizational contributions, several Allies—Poland, Lithuania, the United Kingdom, and Estonia, to name a few—were also engaging Ukrainian SOF through various bilateral and multilateral formats. SOCEUR, in discussions with NSHQ, recognized that without coordination of these efforts, duplication and inefficiencies would impede Ukrainian SOF development.

Recognizing the risk of redundancy, SOF representatives from eight nations, including the United States, convened at NSHQ in November 2017 to design a unified approach to supporting Ukrainian SOF development.³⁵ The group began by simply sharing engagement schedules. As the meeting progressed, participants reprogrammed conflicting events and realigned activities to achieve greater synergy. NSHQ did not have a mandate to compel nations to continue this sort of collaboration, nor did the attendees have the authority to subordinate their national efforts to a collective cause.

Yet the benefit of this cooperative approach was clear to all. The group thus devised the term *multinational SOF advisory team* (MSAT) and unofficially declared that all Allies engaged in supporting Ukrainian SOF development would coordinate via the MSAT mechanism. The MSAT would meet quarterly, along with its Ukrainian SOF counterparts, to analyze progress, synchronize activity, and update the development plan. For its part, NSHQ maintains the mutually agreed SOF development plan and ensures that the plan is linked to the



PARP and CAP. Though imperfect and still evolving, the MSAT approach helps ensure that allied support, including U.S. SOFIB, to Ukrainian SOF development, tactical through institutional, is coherently accounted for and executed.

Within the SOFIB framework of autonomy, joint and interagency integration, operational C2 capabilities, and service-like competencies, the UKRSOCOM transformation highlights the challenges of SOF institutional change. Overall and while still ongoing, the UKRSOCOM transformation shows moderate progress toward the generic SOFIB objectives, albeit over a longer time horizon and with the commensurately longer commitment of U.S. and NATO resources.

For SOF autonomy, despite the naturally occurring organizational friction and inertia, the Ukraine parliamentary



Belgian special forces advise Nigerian soldiers during class on ground movement and attacking an objective, at Camp Po, Burkina Faso, on February 20, 2019, during Flintlock 19 (U.S. Army/Richard Bumgardner)

decision in 2016 provided the necessary political impetus and authority to allow the creation of a true SOF service component, commanded by a general officer. For joint SOF integration, the rebuilding of the 73rd Maritime Special Purpose Center and the development of a SOF air component are multiyear projects, and the construction of joint cooperation and a joint culture is expected to proceed slowly over the years.

In terms of SOF operational C2 capabilities, UKRSOCOM is at a nascent stage, but it has made progress with the NATO certification of a Ukrainian special operations land task group for a future NATO NRF-SOCC under a designated lead nation.³⁶ This Polish and Lithuanian SOF-supported achievement is significant for NATO SOF interoperability; the November 2002 NATO Summit in Prague established the NRF to replace the

Allied Command Europe Mobile Force. The NRF includes land, maritime, air, and special operations components ready for immediate evacuation or crisis response operations around the globe.³⁷ Ukraine's achievement, as part of its SOFIB process, allows it to contribute to NATO missions within the NRF framework.

Finally, UKRSOCOM develops its SOF service competencies steadily through the implementation and application of SOFIB partner advice and the accompanying SC packages in the areas of personnel, training, and equipment. A good example of the latter is the SOCEUR SOFIB advisor recommendation to UKRSOCOM to provide temperature-controlled, weather-resistant U.S. Alaska tents, mounted on concrete pads, to ensure the health and well-being of UKRSOF candidates attempting the SOF qualification course.³⁸

Although weapons may seem more important, the procurement of the tents via SC monies increased the pass rate of Ukrainian special forces operators, which enhanced the overall combat readiness of the organization. For a formation of approximately 6,500 personnel, with fewer than 2,000 operators, force generation plays a significant role for strategic success.³⁹ Yet the provision of these tents raises broader questions about this type of U.S. security force assistance: Is SOFIB using a systems approach for facilities and other DOTMLPF themes? Are the tents merely a one-off transaction or an interim step toward an enduring facilities solution, alongside specific range requirements, roads within the training areas, firebreaks, and other needed infrastructure requirements? Is multiyear funding secured for these developments? Such questions emphasize

the need for a long-term and deliberate perspective for SOFIB and more generic U.S. SFA efforts.

Lessons Learned on SOF Transformation and Implications for Future SFA

The Belgian and Ukrainian SOF institutional transformation cases are representative of a larger SOFIB group of countries and demonstrate five lessons learned for potential future U.S. SFA activities.

There Must Be a Focus on National-Level Organizational Transformation. Political willpower and legal foundations are needed for such change.⁴⁰ A parliamentary decision in the case of Ukraine and a policy-level mandate for Belgium created the necessary legal and policy parameters for SOFIB. The effort is not solely a military activity; hence, it requires a broad range of U.S. advisors—officers, noncommissioned officers, and government civilians—who are both innovative and politically astute.⁴¹ The development of SOCOM-like structures with allies and partners occurs in a dynamic national political-military environment, and U.S. advisors must be cognizant of the political dimensions of such SFA initiatives.

General Officer-Level Sponsorship and Involvement Are Necessary. If flag officer representation is not available, the existing bureaucracy will tend toward inertia and not implement the necessary changes. In both case countries, defense leadership designated an appropriate leader—a major general in Belgium, a lieutenant general in Ukraine—to catalyze the effort. For the United States, this requirement implies a reciprocal general officer focus and commitment over multiple command cycles. The current 2-year rotational command cycle for U.S. general officers is not conducive to such long-term and deliberate SFA initiatives. If changing this rigid U.S. personnel policy is unrealistic, then the general officer transitions need to be better managed to provide continuity for these long-term SFA initiatives.

There Must Be Highly Qualified Joint Staff Officers From All Partner Countries. Selected officers from the

partner country serve as the primary interface with U.S. joint advisory teams. Fortunately, both Belgium and Ukraine selected the best of their joint SOF talent pool to lead their respective efforts. This prerequisite applies equally to the U.S. advisor profile, which needs further refinement. Foremost, U.S. officers who conduct such SFA operations require joint expertise and experience because SOF by nature is a joint force in both the U.S. and foreign contexts. Although the maritime and air SOF components of many allies and partners are underdeveloped, they must be considered in an institutional construct, which requires that the advisors understand how a joint force should function. This situation means that advisors must come to the engagement already fully joint professional military education II-qualified—a condition regularly not met on geographic combatant command and component staffs.

Equally, cross-cultural interpersonal skills and experience are critical for successful advisory communication and relationship development because SOFIB in Europe is often more iterative and collaborative rather than instructional. This observation reinforces the lessons of earlier U.S. advisory experience in the Middle East, which confirmed that cross-cultural competence is crucial for success.⁴² This view also aligns with the DOD description: “An advisor’s primary purpose is to create professional relationships that will inspire and influence their counterparts, and their counterparts’ organization, to become more effective and accomplish their missions, while putting in place sustainable processes that will endure beyond their tour as an advisor.”⁴³

Finally, SC knowledge and project management skills round out the advisory profile. In fact, these latter knowledge areas are often the most challenging to develop. This reflection implies potentially incorporating these themes in core joint professional military education. Another possibility would be to increase the role of the country team SDO or ODC in providing this knowledge. The main

concern with this option is the limited bandwidth of the SDO and ODC for engagements. Particularly in the Ukraine case, the military element of the country team was already managing a large portfolio of programs and activities, and while well informed on the SOFIB activities, its members were not participatory in the process due to other commitments.

There Must Be Design Tailoring. A national SOF institution requires a pattern based on a unique state context and its political-military characteristics; foreign and U.S. models may be useful for the iterative discussion but should not necessarily be replicated.

Due Diligence/Information on Earlier or Parallel Efforts Is Required. As demonstrated by the UKRSOCOM case study, the United States needs to discover, acknowledge, and align with earlier, existing, or potential Allied or coalition efforts ongoing within an SFA initiative to avoid duplication, repetition, or the crowding out of other SFA providers. Rather than taking a unilateral approach, U.S. efforts may work better within a collaborative construct or may not even be needed. In the end, U.S. SFA and the narrower SOFIB are about effective outcomes, not solely actions. This objective requires host nation cooperation and, importantly, U.S. strategic patience.⁴⁴

SOFIB takes on significant importance for the future because as irregular and hybrid warfare becomes more prevalent, the relevance of SOF increases.⁴⁵ Allied and partner nation SOF can be sustainable and operationally effective in a near-peer environment only if they exist within a proper institutional framework. U.S. SOFIB advisory efforts are essential to this objective. SOFIB is also about innovation, which encompasses an alteration of core organizational tasks and is a product of interrelated reforms in personnel management, professional military education, training, doctrine, and modernization. For such change to have impact, it must be embedded and incentivized in the organization’s way of doing business.⁴⁶ Both these aspects also inform changing the broader U.S. SFA

approach from a tactical to institutional focus with the provision of well-qualified advisors, who enable a partner or ally to transform to a more effective military organization. **JFQ**

Notes

- ¹ Jahara Matissek and William Reno, "Getting American Security Force Assistance Right: Political Context Matters," *Joint Force Quarterly* 92 (1st Quarter 2019), 66, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_65-73_Matissek-Reno.pdf.
- ² Anne Tjepkema, "A Dutch SOCOM: The Way Ahead to Addressing National and International SOF Shortfalls," *Atlantisch Perspectief* 42, no. 4 (2018), 19–22.
- ³ Joint Publication (JP) 3-20, *Security Cooperation* (Washington, DC: The Joint Staff, May 23, 2017), v, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_20_20172305.pdf.
- ⁴ *Security Force Assistance Planner's Guide* (Washington, DC: Joint Center for Security Force Assistance, January 1, 2016), 1-1, <https://afghanwarnews.info/documents/JCISFA-SFA-Planners-Guide15Jan2016-CDR-1543.pdf>.
- ⁵ JP 3-20, II-7.
- ⁶ *DOD Dictionary of Military and Associated Terms*, s.v. "Foreign Internal Defense" (Washington, DC: The Joint Staff, November 2021), 87.
- ⁷ Jahara Matissek and Michael W. Fowler, "The Paradox of Security Force Assistance After the Rise and Fall of the Islamic State in Syria–Iraq," *Special Operations Journal* 6, no. 2 (2020), 118–138.
- ⁸ Mara Karlin, "Why Military Assistance Programs Disappoint: Minor Tools Can't Solve Major Problems," *Foreign Affairs* (November/December 2017), 111, <https://www.brookings.edu/articles/why-military-assistance-programs-disappoint/>.
- ⁹ See Stephen Biddle, Julia Macdonald, and Ryan Baker, "Small Footprint, Small Payoff: The Military Effectiveness of Security Force Assistance," *Journal of Strategic Studies* 41, no. 1–2 (February 2018), 89–142; Matissek and Fowler, "The Paradox of Security Force Assistance."
- ¹⁰ Renanah Joyce, Max Margulies, and Tucker Chase, "The Future of U.S. Security Force Assistance," *Modern War Institute*, November 23, 2021, <https://mwi.usma.edu/the-future-of-us-security-force-assistance/>.
- ¹¹ Matissek and Fowler, "The Paradox of Security Force Assistance," 128.
- ¹² *Ibid.*, 126.
- ¹³ Jahara Matissek and Austin Commons, "Thinking Outside of the Sandbox: Succeeding at Security Force Assistance Beyond the Middle

East," *Military Review* 101, no. 2 (March–April 2021), 37.

- ¹⁴ Jerad Harper, "A Tug of War for Effectiveness: U.S. Efforts to Build the Republic of Vietnam Armed Forces (1955–1973)" (Ph.D. diss., George Mason University, 2021), 27.
- ¹⁵ Tjepkema, "A Dutch SOCOM," 19–22.
- ¹⁶ The author formulated these special operation forces (SOF) institution-building objectives as part of the iterative advisory process with the Belgian SOF project team.
- ¹⁷ *The Strategic Vision for Defence*, ed. Renaud Flamant and Pieter-Jan Parrein (Brussels: Ministry of Defence, 2016), 23–35, <https://cyberwar.ro/wp-content/uploads/2018/10/strategic-vision-belgian-defense-en.pdf>.
- ¹⁸ *Ibid.*, 50–51.
- ¹⁹ Alexander Mattelaer, *Why Belgium Needs a Special Operations Command*, Security Policy Brief No. 70 (Brussels: Egmont Royal Institute for International Relations, April 2016), 5.
- ²⁰ *The Strategic Vision for Defence*, 122–123; Nathan Gain, "A Belgian Special Operations Command," *Forces Operations* (blog), July 25, 2016.
- ²¹ Tom Bilo, "SOF in Great Power Competition: The Belgian Perspective," June 30, 2020, *The Politics of Special Forces* podcast, produced by Christian Breede and Kevin D. Stringer.
- ²² "Belgium SOF Directorate Legal Proposal," undated.
- ²³ "The Belgian Army Inaugurated Its Special Operations Regiment," *Army Recognition*, July 4, 2018, https://www.armyrecognition.com/july_2018_global_defense_security_army_news_industry/the_belgian_army_inaugurated_its_special_operations_regiment.html.
- ²⁴ Tom Bilo, "Strategic Vision 2030: Development of a BEL Special Operations Command" (presentation, Garmisch-Partenkirchen, Germany, November 4, 2016); "The Belgian Army Inaugurated Its Special Operations Regiment."
- ²⁵ Tom Bilo (director, Belgian Special Operations Command), discussion with the author, June 2021.
- ²⁶ Tom Bilo, "BELSOF: Quo Vadis?" *The Kingston Consortium on International Security Insights* 1, no. 6 (July 2021), <https://www.thekcis.org/publications/insights/insight-16>.
- ²⁷ Bilo, "SOF in Great Power Competition."
- ²⁸ Christopher Lamb, "Global SOF and Interagency Collaboration," *Journal of Strategic Security* 7, no. 2 (Summer 2014), 8–20.
- ²⁹ Bilo, "SOF in Great Power Competition."
- ³⁰ Andrii Biletskyi, "Today's Ukrainian Special Operations Forces" (presentation, Ukrainian Special Operations Forces Command, 2020).
- ³¹ *Ibid.*
- ³² "Ukraine's Parliament passes law 'On amendments to some laws of Ukraine on Special Operations Forces of Armed Forces of Ukraine,'" Ministry of Defence of Ukraine, July

7, 2016; Illia Ponomarenko, "Combat Hardened Special Forces Officer Vows to Reform UkrOboronProm," *Kyiv Post*, April 17, 2019, <https://www.kyivpost.com/ukraine-politics/combat-hardened-special-forces-officer-vows-to-reform-ukroboronprom.html?cn-reloaded=1>.

- ³³ Byron Harper (deputy director for partnership, NATO Special Operations Headquarters), in discussion with the author, December 2021.
- ³⁴ *Ibid.*
- ³⁵ *Ibid.*
- ³⁶ "Ukrainian SOF Joins International SOF Family," Ministry of Defence of Ukraine, June 27, 2019.
- ³⁷ "Prague Summit Declaration," NATO Press Release 127, November 18, 2002, <https://www.nato.int/docu/pr/2002/p02-127e.htm>.
- ³⁸ "SOF Training Center Received the Most Modern Tent Camp," Ministry of Defence of Ukraine, February 24, 2020; Kirk Smith (commanding general, U.S. Special Operations Command Europe), remarks, U.S. Embassy Kyiv, February 24, 2020, <https://ua.usembassy.gov/remarks-by-major-general-kirk-smith-commander-of-u-s-special-operations-command-europe/>.
- ³⁹ U.S. Special Operations Command Europe Public Affairs Office, e-mail response to *New York Times* query, October 21, 2019.
- ⁴⁰ Implied in Matissek and Reno, "Getting American Security Force Assistance Right," 71–72.
- ⁴¹ Edward Ballanco, "Security Force Assistance Needs the Stillwell Combination," *War Room*, May 24, 2019, <https://warroom.armywarcollege.edu/articles/security-force-assistance-stilwell-combination/>.
- ⁴² Paul Szostak and Juan Pizarro, "Strategic Expeditionary Advising: Exploring Options Beyond Afghanistan–Pakistan Hands and Ministry of Defense Advisors," *Air Force Journal of Indo-Pacific Affairs* 2, no. 4 (Winter 2019), 4, https://www.airuniversity.af.edu/Portals/10/JIPA/journals/Volume-02_Issue-4/Szostak.pdf.
- ⁴³ Center for Army Lessons Learned Handbook No. 19-06, *Advising at the Senior Level: Lessons and Best Practices* (Fort Leavenworth, KS: Center for Army Lessons Learned, January 2019), 6, <https://usacac.army.mil/sites/default/files/publications/19-06.pdf>.
- ⁴⁴ Mark Davis, "Defense Institutional Building in Post-1999 NATO Nations: Lost Opportunity in SOF Development" (unpublished white paper, 2015).
- ⁴⁵ Mattelaer, *Why Belgium Needs a Special Operations Command*, 4.
- ⁴⁶ Suzanne Christine Nielsen, "Preparing for War: The Dynamics of Peacetime Military Reform" (Ph.D. diss., Harvard University, 2003).



U.S. Army Soldiers assigned to Bravo Company, 2nd Battalion, 87th Infantry Regiment, 2nd Brigade Combat Team, 10th Mountain Division, and Chilean army soldiers assigned to 3rd Mountain Division, cross-country ski at Chilean Army Mountain School in Portillo, Chile, August 27, 2021 (U.S. Army/ Joshua Taeckens)

Analyzing a Country's Strategic Posture

Suggestions for Practitioners

By Beatrice Heuser

Diplomats and defense attachés when posted to a country are expected to give a fresh

Professor Beatrice Heuser holds the Chair in International Relations at the University of Glasgow and teaches strategy at the Führungsakademie (Military Staff College) of the Bundeswehr.

assessment of that country's strategic posture. The term *strategic posture* is used here to encompass not only the country's military—personnel, equipment, bases, and other infrastructure—but also its political-strategic alignment (friendly? neutral? potential rival/adversary?), its overall attitude to war, and its spirit (as one used to say), or collective

culture and mentality. The utility of this exercise is that, if done prudently and with an eye for nuance, it has some predictive value. Even the world's only superpower has an interest in judging what positions other governments may take in a dispute. Beyond predictions—which can only ever be very short-term, a year or so at best—one can identify

some potentialities, that is, possible future developments that may or may not come to pass. For example, in a country where governments are elected, the victory of a party or coalition with attitudes to particular conflicts and international alignments different from those of the present government may come to dominate.

Such analysis is crucial for the determination of one's own larger overall strategy and, as a part of that, one's approach toward this country and its government. Even in World War II, when the United States had reached the height of its military power, it had to make strategic choices. Would it prioritize victory in Europe or victory in the Far East? Influenced by its European allies and estimating that Europe was the more precious and important theater of war, America chose the former. Today, too, similarly grand strategic choices have to be made not only by America but also by second- and third-tier powers. To do so, strategic decisionmakers need to understand and, to some extent, predict the postures of other players.

Several attempts have been made by leading scholars to identify the various dimensions that need to be explored to come to a comprehensive understanding. As early as the late 19th century, Alfred Thayer Mahan had a list of factors that would determine whether a country and its population were “naval-minded”: to be a sea power, he argued, one needed to have an advantageous geographical position; “serviceable coastlines, abundant natural resources, and favorable climate”; a sizable territory and a population large enough to defend it; a naval-minded society (one with “an aptitude” for navigating the seas and for commercial enterprise); and a “government with the influence and inclination to dominate the sea.”¹ Colin Gray explores 17 dimensions of strategy in his book *Modern Strategy*, divided into three categories: “People and Politics,” “War Preparation,” and “War Proper.” “People and Politics” covers individual leaders, society, culture, politics, and ethics. “War Preparation” includes the economy of the country concerned, logistics (implicitly also

geography—logistics from where to where), the organization of the armed forces and their administration, information and intelligence, strategic theory and doctrine, and technology.²

A very insightful research project carried out by Valerie Hudson at Brigham Young University in 1998–1999 looked at foreign policy action templates. She and her teammates conducted opinion polls in the United States, Russia, and Japan to establish how respondents thought their governments would act in certain crisis scenarios—what strategic postures they would assume—and how they thought the other two governments would react. The outcome was a remarkable convergence of predictions (obviously, not confirmed by real events). Hudson applied the premise that the governments of states will approach decisionmaking in crises with “a preestablished set of . . . behavioral dispositions,” “a repertoire or palette of adaptive responses,” and “off-the shelf strategies of action.” She maintains that these are cultural responses to any given situation. The interest of her study lies in the fact that the responses may yield some element of “predictability to international interactions.”³ Her study relied on what I call the principle of corresponding vessels: namely, that in relatively open societies (and Russia was relatively open in the late 1990s), actions governments think they can take have a strong connection with what they think their electorates will support and alert observers outside government—journalists, academics, attentive readers of good news media—have a sense of what their governments are likely to do.

Mine is a different take, which focuses precisely on the whole list of factors that influence a state's strategic *posture*, giving due attention to both hard and soft factors, the former most emphatically including geography and available means, the latter including strategic culture and collective mentality. Soft factors are very much influenced by hard factors, and yet the results are specific to different cultures. Culture will influence a society's (and its government's) outlook on the world, simplified according to its

myths and narratives, its “mentality”; it will influence the society's preferences when it comes to making strategic decisions, discounting or proposing options according to historical experiences and precedents that are seen as constituting analogies. Indeed, we shall see that ideas with their own roots in diverse cultures, distinct historical experiences, and equally distinct interpretations in turn influence many of the analytical dimensions identified, mixing with hard factors in ways specific to each state and its populace. To repeat, the purpose of my approach is not only to allow some very short-term predictions but also to indicate key alternatives of potential future developments. This goal can be accomplished by enquiring into both hard and soft (cultural) factors that make up a country's strategic posture.

Geography, Resources, Economy, and Trade

The most enduring hard factors are a country's geography, its natural resources, and, to a large extent as functions of these, its economy and what it can export and needs to import. The most enduring is geography, which, as Colin Gray puts it, “is ‘out there’ objectively as environment or ‘terrain.’”⁴ But even geography changes: rivers and ports silt up and may cease to be shippable; the course of rivers has been changed by human endeavor; canals have been dug to link up waterways; mountains that it would take days or weeks to climb and descend have been penetrated by tunnels; people have fought back the sea and created new land; lakes have dried up; sea levels have risen and fallen and are now rising dangerously again.

Yet geography, as Geoffrey Sloan and Colin Gray put it, is the “mother of strategy.”⁵ Technology can only mitigate the conditioning power of geography. An island in the Pacific does not have to worry about waves of immigration from Africa or the Middle East, but then again, until 2021, we would not have expected refugees from Syria to be attempting to cross into Poland from Belarus, thanks to air transport.

The strategic importance of a geographic location continues to be considerable. Extremely mountainous Switzerland and Nepal and Tibet, although hypothetical thoroughfares, have generally been left alone as too difficult to conquer. But it is not only a country's internal geography but also its location in relation to other powers that makes it interesting or uninteresting to them. In turn, mere geographic proximity to a Great Power will result in its considerable influence on a smaller power, whether this be through peaceful trade (likely to come along with a spreading of trading norms from the larger to the smaller power) or less benign means. A remote, isolated island or archipelago is *prima facie* less attractive to expansionist neighbors than a fertile strip of adjacent land. Yet the former can still become a bone of contention. Owning a remote island can translate into commanding a naval base. And a remote island can be of considerable interest to other powers because of rare natural resources. Inhospitable or remote areas can also be of importance to other powers as thoroughfares if they are flat—thus, both the great Central Asian steppes and small Flanders were for centuries passageways for armies on their way to war and conquest.

Natural resources condition the economic productivity of any country. Are its lands large and fertile enough to feed its population? If not, does it depend on imports from another country (which gives that other country political leverage)? Are the resources available for industrialization? How far has industrialization (or a postindustrial restructuring of the economy) progressed? What indigenous industrial products are there? What is the structure of industry—does it rely on the import of raw materials, or on foreign investment or exports? Both, of course, imply an important interdependence with sources of raw materials and with markets for goods. Answers to these questions will help to ascertain interests—often unarticulated—that condition a country's strategic posture. Can it even afford to take a position against a foreign power that has heavily invested in its economy, or on which it depends for fuel or gas imports? Amassing an army at the borders

of another country is not the only way to exercise strategic leverage over it.

Population

Economic factors overlap greatly with the demographics of a country. Is the country populous? What is the density of settlement? Is there overcrowding? What are employment rates? Do many workers seek work in other countries? Could they potentially be held hostage? And does the economy depend on workers abroad sending back their savings?

Alternatively, is there a substantial proportion of foreign workers in its economy whose principal allegiance is to their original polity or who might be vulnerable to blackmail if they have left behind family? Even without the import or export of labor, there might be tensions arising from a minority in one country (a diaspora) that is ethnically closer to the population of another and that might be willing to fight for its independence or separation from one country and integration into the other. There might be diaspora allegiances with countries farther away—we have not yet quite seen to what extremes that could lead. The country itself might contain two or several distinct ethnic groups with truly different languages and pronouncedly different traditions, obstructing nation-building and the construction of a larger national identity. Religious differences were and are still dynamite in many countries; the 18th-century wit Georg Christoph Lichtenberg commented that people seem to find it easier to kill others to promote their own religion rather than live according to its rules.

Related are questions about the demographic structure of the society. Are workers poorly, moderately, or highly skilled? Is there an unemployed youth bulge (often associated with bellicosity⁶), or are there more old people (making the society tendentially pacific) dependent on government pensions and medical resources, including perhaps care workers from abroad? Regardless of their actual allegiances, a foreign labor force may encounter xenophobia. Is such xenophobia being exploited

by demagogues? Are there other frustrations in the population that lend themselves to such political exploitation?

Constitution and Powers

The political constitution of a country is the product of historical developments; it generates a formal structure, behind which there may lurk an informal one. A country's formal constitution includes governmental structures; the processes by which governments come to power, are held accountable, and are replaced; the processes by which they operate; and the way and degree to which they are enshrined in formal rules. Is the country formally and *de facto* a democracy with multiple political parties and free elections? In the Cold War, Communist East Germany notionally had opposition parties, which ritually scored around 10 percent of the vote each, but equally ritually in parliament supported the largest party—the Socialist Unity Party—and the Trade Unions Party.

If a country is a democracy, is it a relatively mature, robust democracy? Even such states are vulnerable to demagoguery, as recent years have shown. Are there a free press and free public debate? Are there organized citizens groups, and are there rules according to which they can lobby parliament or the government for a particular cause? How independent and free from corruption is the legal system? Alternatively, is this some form of authoritarian system? Is the government above the law—are legal obligations to which the state has signed up at one point disregarded at another?

Is there a smoothly working legal system? Does the average citizen have faith in the police and judiciary? Or is there a parallel, Mafia-style system that not only is a protection racket but also fills gaps in social welfare for its own that the state does not address?

Behind the constitutional distribution of powers, do economic powers exercise strong political influence? In the past, these would have been large landowners; now such forces are more likely key industries and investors. Are these international actors, or do they perhaps use their influence on behalf of other states? Other elites that



KC-46A Pegasus tanker aircraft from Air Force Reserve Command's 931st Air Refueling Wing refuels Finnish F/A-18, demonstrating U.S. European Command's commitment to bolstering security on NATO's eastern flank in Poland, April 13, 2023 (Courtesy Finland Air Force)

might exercise power informally might include criminal individuals and organizations, indigenous or foreign or a mix.

Armed Forces

The political system of a country also determines the structures and recruitment processes of its armed forces. The size of these forces depends on not only the population base but also many other factors. Both threat perception and political ideas germane to a country determine whether it has a purely professional army or a mix of professional cadres and conscript forces; the collective mentality of the nation in question—its inherited ideas on the subject—plays a great part. Does a pacifist tendency prevail that is strong enough to argue against all military service? Is there a tradition of neutrality? Such a tradition may go along with a determined commitment to self-defense. Is a high respect for

the country's own professional forces coupled with the conviction that a free society cannot tolerate compulsory military service? Many other permutations are possible.

For a host of reasons, ranging from alliance treaties to historical legacies, there may be foreign forces stationed in a country, or the country may station some of its own forces abroad (in its colonies or dependencies, in friendly countries, or as part of a postwar occupation), temporarily or more long term. Are these forces and their bases potential or intended launch pads for strategic operations far from home (expeditionary war, *opérations extérieures*)? Again, these are important factors conditioning a country's strategic posture.

A military's equipment of course depends on its means, but the issue also has alliance dimensions. Have larger allies supplied it with secondhand or with state-of-the-art equipment? Is it able to

service and maintain its weapons systems without outside help? Has the equipment a high degree of compatibility with that of other countries? These countries might today not even be allied to the country that originally supplied their arms: ex-Warsaw Pact countries long had to work with equipment inherited from the Soviet Union. In the Gulf War, Iraq's air force included aircraft previously bought from France, creating something of a handicap for France's operations in the coalition.

Then there is a clear overlap with geographic factors, too. Does the country have coastlines, so that it can be a naval power? Does it have mountains and forests and, therefore, inhabitants inclined to specializations like those of the Canadian Mounties, or the *chasseurs alpins*, *Gebirgsjäger*, or alpinists of Europe? What makes up the culture, traditions, ethos, and morale of the military, and to what extent does the military have experience with actual live operations?

Marines with Marine Light Attack Helicopter Squadron (HMLA) 773, 4th Marine Aircraft Wing, Marine Forces Reserve, in support of Special Purpose Marine Air-Ground Task Force Unitas LXIII, conduct flight operations near Christ the Redeemer statue at Corcovado Mountain, Rio de Janeiro, during exercise Unitas LXIII, September 12, 2022 (U.S. Marine Corps/Jonathan L. Gonzalez)





Historical Experiences

The question about the experience of war also concerns the population as a whole, and it leads straight to the enormous role played by a large swath of historical experiences in a collectivity's mentality, or strategic culture in its wider definition.⁷ These can fall into several categories, including direct experience of external wars within living memory (war experienced in one's own lifetime or in the lifetime of older generations that one has overlapped with). Such a war or wars may or may not have affected the homeland itself (and this makes a huge difference, of course). Again, within living memory, any direct experience of internal/civil wars will have a great deal in common with experience of an external war on one's soil.

A distinction between external war and civil war cannot always be made. Often enough, parties to a civil war or insurgency (civil war might be defined as a generally more symmetric form of insurgency) have support from external powers, whereas many conflicts that started as inter-state conflicts have been "internalized."⁸

Every individual survivor of war will have his or her own story, an experience of suffering or being spared, but wars will to a greater or lesser degree involve whole collectives, and this degree matters. Especially, the experience of occupation will have affected entire populations. The experience can be benign, such as the German experience of the American, British, and French military presence since 1945, which turned from resented occupation to welcome allied stationing, or it can be extremely brutal, such as the Soviet experience of the Wehrmacht's occupation in 1941–1944. Conversely, a country's experience of having occupied another may also mark it; for example, many Britons have a deep nostalgia for India, whether or not they themselves have ever visited it. Americans seem to have come away from some occupation experiences abroad benignly inclined toward the locals, whereas others left them deeply scarred.

Historical or traditional enemy images passed along over several generations may have some power, especially if used adroitly by political forces. Thus,

although people living today in Eastern Europe have no personal experience of occupation by the (Muslim) Ottoman Empire, which came to an end in 1922, the aversion of Poland, Hungary, Romania, and Bulgaria to taking in large numbers of Muslim immigrants during the crisis of 2015–2016 can be explained in good part by centuries of fear of the Islamic conquerors. Similar observations can be made about how a culture views war and peace (including neutrality). Until 2022, Sweden was, and Switzerland still is, exceptionally good examples of this proposition; their direct experiences of war and defeat date back a good 200 years and yet wedded them to the creed that neutrality alone is good for them.

Some cultures are prone to see war as a transposition to Earth of a cosmic fight of good against evil, one in which the enemy is evil (and with evil there can be no reconciliation), rather than a political quarrel that has gotten out of hand (as was so often the case in wars of dynastic succession) and that can be settled amicably in a peace treaty. With some enemies, such as Hitler's Nazi Germany, there can be no compromise. Traditions might blind a culture to the possibility that with others, there can.

Culture, Values, and Worldviews

The legacy of great leaders (real or mythical) and their worldviews can also play a role in fashioning societal views—which brings us to other sources of culture, values, and worldviews. Such leaders may be prophets, religious leaders, or mythical heroes such as Rama or King Arthur. Religions themselves are of course of very considerable importance. But there again, any inquiry must keep in mind the contradictory strands *within* religions. Many religions seem to have a more pacific and a more bellicose strand. Think of Christianity: although Jesus himself said nothing at all about war, his love of metaphors left a legacy that can be interpreted either way, "turn . . . the other cheek" versus "He who is not with Me is against Me."⁹ Accordingly, the pacifically minded among his fol-

lowers and the more bellicose created competing traditions. The same is true of Judaism and Islam.

Extinct religions can have a lasting effect on a polity. Medieval West European Christendom, for example, was strongly influenced by the Germanic warrior cults—which explains the great respect paid to the martial upper classes. Epics, myths, and other forms of literature passed on from former generations are of considerable importance; the blood-thirsty heroes of Germany's *Song of the Nibelungs*, England's *Beowulf*, and indeed the much older stories of the Trojan War (or the records of the conquests of Alexander the Great) competed with efforts by the medieval church to limit war. Myths can include views of the world and how it works: is it seen as an anarchy, a world in which *homo homini lupus est*—man is the wild wolf out to eat another man—or as a trading place where all sides can win from peaceful intercourse? Myths include subjective self-perceptions that may greatly skew historical facts, cast a nation as an eternal victim when it has historically repeatedly been the aggressor, or cast a country that has for millennia been inextricably involved in the economy, migrations, and cultural and political developments of its adjacent area as "separate."¹⁰ Another nation that is still remembered by neighbors for its aggressiveness in centuries past can think of itself as firmly and pacifically neutral, even if its government has secretly worked closely with others in matters of defense.¹¹

All these dimensions will be results of the collective mentality of a population (or its collective culture, as others would phrase it). The great French historian of international relations Jean-Baptiste Duroselle defined *collective mentality* as the relatively stable attitudes of mind, or mindsets, images, and stereotypes shared by a group, which contain their own value judgments or echo the value judgments of others. Although doctrines (what is taught by an authoritative institution such as a church) and coherent philosophies, ideologies, or religions might leave their imprint on such a mentality, it tends to be a cluster of beliefs that is not logically coherent.¹²



Navy's newest *Arleigh Burke*-class guided-missile destroyer, USS *Lenah Sutcliffe Higbee*, sits at Naval Air Station Key West's Truman Harbor ahead of her commissioning ceremony in Key West, Florida, May 8, 2023 (U.S. Navy/Nicholas V. Huynh)

All such factors also condition the ways international relations are viewed overall. Does a culture view peace or conflict as the norm? Is peace even seen as desirable? Even looking just at Europe, we find both traditions going back a long way: there is the intrinsically pacifist one, but there is also one that sees peace as furthering decadence, softness, and selfishness, and war as good, as bringing out a civic spirit of self-sacrifice and solidarity.¹³

Adversaries and Their Strategic Ambitions

Now add to this mix not just *perceptions* of (actual or potential) adversaries but also their strategic ambitions. The

actions of a neighbor or nearby power will affect any government's strategic posture. Even the most defensive military buildup tends to be seen as potentially threatening by neighbors, as the famous "security dilemma" paradigm explains. There will be knock-on effects if any one state in a region begins to build up its forces, acquires new weapons and platforms, or reconfigures its fighting power without coordination through a military alliance. A bully throwing its weight about in a region, or even directly threatening or coercing a third power into behavior it sought to resist, will unnerve other powers, and they will reconsider their strategic postures.

Even nonmilitary measures can play a considerable part. A power coercing another into a trade agreement or into opening or closing its market to certain goods, or expelling foreign workers or enticing them into its workforce in what might amount to a brain drain—all these actions will have strategic repercussions in one form or another—will be feared, resented, or more influential, as dependence is created or increased.

Alliances and Obligations

In the context of such developments, a government is likely to look around for partners or allies—"like-minded" countries. This brings us to the country's atti-



From left, USNS *Charles Drew*, USS *Comstock*, USS *Shiloh*, USS *New Orleans*, USS *Chicago*, USS *America*, USS *Ronald Reagan*, USNS *John Ericsson*, USS *Antietam*, USS *Germantown*, and USNS *Sacagawea* steam in formation while E/A-18G Growlers and FA-18E Super Hornets from Carrier Air Wing (CVW) 5, P-8 Poseidon from Commander Task Force 72, and Air Force F-22 Raptors and B-1B Lancer fly over formation in support of Valiant Shield 2020, Philippine Sea, September 25, 2020 (U.S. Navy/Codie Soule)

tude to alliances, contractual obligations, and membership in international organizations. Such membership formally conditions many interactions with other polities' militaries and will result in a degree of (often mutual) acculturation, at least among the military and other professionals through joint exercises and joint work in various units. How allies are perceived is a thing of infinite complexity, however, and multiple factors play a role.¹⁴ In the Cold War, the propaganda effort and sheer pressure from above needed to turn the alliance between three traditional enemies—Russia, Poland, and Prussia/East Germany—into a “brotherhood in arms” (thus the name of Warsaw Pact joint military exercises) must have been

considerable. Other paradoxes persisted: the enormous admiration of Western European cultures—especially among the young—for the United States could bring forth the American-jeans-wearing anti-American protesters who troubled European capitals of 1968–1972, inspired by the anti-Vietnam demonstrations on American university campuses. It is also notable how older perceptions can survive decades of closest cooperation as allies: the Franco-British *entente cordiale* can still be rocked by fishermen's disputes that give rise to media references to centuries of sibling rivalry, and British reactions to the German unification in the early 1990s revived memories of competition and war, 1870 to 1945.

All of Which Interact

All these factors will also color the ways individual cultures perceive a larger political situation, but finer insights are required to understand which way a polity will turn, given often counterbalancing or contradictory influences. For example, *despite* its now 200-year-old tradition of neutrality and widespread pacifism, Sweden, alone among Russia's European neighbors, has reintroduced national military service in response to a perceived revived Russian threat. *Because* of their perceptions of the role of the military in society, and in accordance with their country's neutrality, a majority of Aus-



trians voted to retain national military service—in this case nothing to do with Russia. *Despite* its membership in the North Atlantic Treaty Organization but *because of* its widespread pacifism, Germany, the last European Union member state to abolish conscription (in 2011), has not since seriously debated its reintroduction.

These few examples serve to illustrate the way multiple factors come together, some balancing each other out, others reinforcing each other, to influence big decisions about strategic postures—aided, no doubt, in good measure by the inertia congenital to all bureaucracies. Nevertheless, this list of factors may serve as useful guidance for exploring different and interactive dimensions of a state's political and social makeup, its resources and economic means, its armed forces and their hardware, its culture or cultures, its

allies and foes and feelings about them, its views on war and peace. The diplomatic and intelligence communities require such assessments. Their results will allow more informed and educated guesses about the range and limits of policies and strategies that governments of individual states can and probably will pursue, and about the themes likely to surface or be passed over in silence in big public debates about questions of war and peace.

Conclusions

To conclude and repeat: a country's strategic posture is a function of multiple factors, many of them interdependent—whose effects on one another can be linear or nonlinear, positively strengthening or counterbalancing. Any country's strategic posture depends much on context and will be successful or unsuccessful depending on context. Belgium's neutrality did not protect it from aggression either in 1914 or in 1940, positioned as it was between two large combatant parties. By contrast, whether Singapore and Malaysia, with their geographic positions crucial to international navigation, can retain their nonaligned status in the coming decades depends on the evolution of their unsteady region. And yet, notwithstanding the utility of a particular stance, the culture and historical experiences of a country may well move its government to favor a posture that does not work to its objective advantage. It may discount options and narrow its choices. Thus, both hard factors—geography, means, resources—and soft factors need to be included in any analysis.

What is outlined above is designed to facilitate the practitioner's analysis of a government's or a country's strategic posture. Some of the factors for analysis are immutable, especially geography, although climate change affects even this hard factor. Others are in constant flux. And yet taken together, all these dimensions can offer some useful estimates crucial to one's own strategic decisions. This is the job of diplomats and defense attachés, who will, it is hoped, find this little article useful for their purposes. JFQ

Notes

¹ Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660–1783* (Boston: Little, Brown, 1890), 25–89.

² Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 20–24.

³ Valerie M. Hudson, “Cultural Expectations of One's Own and Other Nations' Foreign Policy Action Templates,” *Political Psychology* 20, no. 4 (December 1999), 767–768, <https://www.jstor.org/stable/3792194?seq=10>.

⁴ Colin S. Gray, “Inescapable Geography,” in *Geopolitics, Geography, and Strategy*, ed. Colin S. Gray and Geoffrey Sloan (Abingdon, UK: Routledge, 2014), 163.

⁵ Colin S. Gray and Geoffrey Sloan, “Introduction,” in Gray and Sloan, *Geopolitics, Geography, and Strategy*, 3.

⁶ Henrik Urdal, “A Clash of Generations? Youth Bulges and Political Violence,” *International Studies Quarterly* 50, no. 3 (September 2006), 607–629.

⁷ Beatrice Heuser, “Historical ‘Lessons’ and Discourse on Defence in France, Germany, 1945–1990,” *Rethinking History* 3 (July 1998), 199–237.

⁸ International Institute for Strategic Studies, *Armed Conflict Survey 2021* (Abingdon, UK: Routledge, 2021), fig. 1 (Global Conflict Trends).

⁹ Matt. 5:38–42, 12:30.

¹⁰ Antonio Varsori, “The Myth of British Separateness,” in *Haunted by History: Myths in International Relations*, ed. Cyril Buffet and Beatrice Heuser (Oxford: Berghahn Books, 1998), 134–156.

¹¹ Ann-Sofie Dahl, “The Myth of Swedish Neutrality,” in Buffet and Heuser, *Haunted by History*, 28–40.

¹² Jean-Baptiste Duroselle, “Opinion, attitude, mentalité, mythe, idéologie: Essai de clarification,” *Relations internationales*, no. 2 (1974), 3–23.

¹³ Beatrice Heuser, *War: A Genealogy of Western Ideas and Practices* (Oxford: Oxford University Press, 2022), 67–80.

¹⁴ See Beatrice Heuser, *Nuclear Mentalities? Strategies and Beliefs in Britain, France, and the FRG* (London: Macmillan, 1998).



General Laura J. Richardson, commander of U.S. Southern Command, delivers remarks at Women, Peace, and Security roundtable as part of Continuing Promise 2022, in Cartagena, Colombia, November 13, 2022 (U.S. Navy/Sophia Simons)

Integrating Women, Peace, and Security Into Security Cooperation

By Barbara Salera

Security cooperation (SC) programs—or Department of Defense (DOD) activities “to build and develop allied and friendly

Dr. Barbara Salera is an Assistant Professor at Defense Security Cooperation University.

security capabilities for self-defense and multinational operations . . . provide the armed forces with access to the foreign country . . . [and] build relationships that promote specific United States security interests”¹—are one of the most widely used tools the United States has at its disposal to achieve national secu-

urity and foreign policy objectives. Each year, the United States transfers billions of dollars’ worth of weapons, training, and credit to foreign countries to help build partner-nation militaries in service of achieving American interests.²

The success of using SC to achieve national security objectives or to build

partner-nation military capacity, however, remains uneven even under the best of circumstances.³ For SC activities in partner nations to achieve results the United States seeks, all segments of society must be included. Currently, the benefits of SC programs fall disproportionately on male members of partner-nations' militaries.⁴ Not only are women excluded, they are often perceived as passive observers or victims of insecurity as opposed to thinkers and actors involved in ensuring a nation's security.⁵ As a reflection of American values, women should have equal access to the benefits of SC and other U.S.-provided assistance programs and need to be included in wider peace and security efforts. As Anne Witkowski has argued, when women are included, they "enlarge the scope of [peace] agreements to include the broader set of critical societal priorities and needs required for lasting peace."⁶

Integrating women into peace and security operations can also act as a force multiplier in the planning and execution of these activities.⁷ There is a reason that even traditionally conservative terrorist organizations, such as Boko Haram, often recruit women as suicide bombers.⁸ Women, especially in conservative societies, have access to people and places that men may not.⁹ In addition, because of a focus on male power centers, women's value and power in paternal societies are often overlooked, to the detriment of military operations.¹⁰ Gendering analyses and integrating women into SC planning will widen the scope of what is possible to accomplish. Without a complete understanding of the context of a conflict, it is difficult for a military organization to establish objectives, much less identify the means to accomplish them. Robert Egnell argues that "gendered dimensions of conflict can indeed be tremendously transformative by affecting *both* what the operation does and *how* it does it, in terms of its priorities and tactics."¹¹ Finally, women need to be integrated into security sector activities just as a matter of building a more representative, responsive, legitimate, accountable, and democratic government.¹² The Joe Biden administration's National Security

Strategy clearly makes building "an inclusive world" an important objective, reinforcing the need to expand the scope of security cooperation to include women to achieve this end.¹³

In widespread recognition of the benefits of female inclusion in peace and security issues, on October 31, 2000, the United Nations (UN) unanimously passed UN Security Council Resolution (UNSCR) 1325 on Women, Peace, and Security (WPS).¹⁴ This resolution recognized the importance of women in advancing peace and security. The passage of UNSCR 1325 highlighted the influence nongovernmental organizations (NGOs) can have on introducing and institutionalizing norms of behavior on an international scale.¹⁵ The passage of UNSCR 1325 has had a profound effect on member states, which were urged to integrate gender perspectives into peacekeeping operations,¹⁶ to invite gender training "into their national training programmes for military and civilian police personnel in preparation for deployment,"¹⁷ and to develop national action plans (NAPs), which structure the implementation of a WPS "regime" at the country level.¹⁸

One of the earliest countries to develop a NAP was Denmark, which created its plan in 2005, followed by Norway, Sweden, and the United Kingdom in 2006.¹⁹ The United States did not develop and release its NAP until 2011, when many countries, such as the United Kingdom, were already busy refining theirs.²⁰ Between 2000 and 2020, the UN implemented WPS objectives through gender balancing, which seeks to increase "the number of women in a given role" and through a practice known as gender mainstreaming. According to the UN Entity for Gender Equality and the Empowerment of Women, gender mainstreaming is a "strategy for promoting gender equality . . . [that] involves ensuring that gender perspectives and attention to the goal of gender equality are central to all activities—policy development, research, advocacy/dialogue, legislation, resource allocation, and planning, implementation and monitoring of programmes and projects."²¹

In 2017, under the Donald Trump administration, the United States sought to institutionalize its NAP when Congress passed Public Law 115-68, *The Women, Peace, and Security Act*. This legislation has been touted as "the first legislation of its kind globally"; it seeks to incorporate the priorities of the WPS agenda into law.²² The WPS Act of 2017 specifically requires "relevant Federal agencies" to formulate a coordinated strategy and implement integrating WPS objectives into various activities. The National Defense Authorization Act for fiscal year 2020²³ further reinforces the WPS framework by legislating that DOD incorporate "gender perspectives and participation by women in security cooperation activities to the maximum extent practicable."²⁴ In 2022, DOD spent approximately \$5.5 million to hire personnel, establish policies, and integrate relevant training for WPS into professional military education institutions, with an additional \$3 million for SC activities.²⁵

With the WPS framework now having the weight of law, SC planners and practitioners must consider how to integrate its requirements into activities. Military planners often look to doctrine for guidance on how to accomplish objectives, but as currently written, joint doctrine does not provide adequate guidance on integrating a gendered analysis into planning.²⁶ Although Joint Publication 5-0, *Joint Planning*, mentions "gendering analysis" as an important aspect of depicting the operational environment, it gives no further guidance. It may be an assumption that a gender advisor (GENAD) would conduct this analysis. Many combatant commands do have GENADs on staff to assist in integrating WPS objectives, but even those tasked to serve may have limited experience.²⁷ As one GENAD put it, being tasked often falls on the "nearest woman" and is in addition to her regular duties.²⁸ Such a process further confuses what GENADs are to do, other than advocate for or consider women's rights and increase the number of women participants (often referred to as gender balancing), as opposed to conducting a gender analysis.

This article provides a quick overview of WPS guidance documents and provides some insight on how to integrate WPS objectives into SC planning and activities through use of gender mainstreaming to both ensure gender balancing and conduct a gender analysis. Integrating WPS objectives into SC activities is not only mandated; it is also key to ensuring SC objectives have the intended effects on achieving interoperability and long-term global security and regional stability.

An important point to reinforce is that while the phrase *women, peace, and security* singles out *women*, it is important not to think of achieving WPS objectives as simply a women's issue. WPS objectives are human rights objectives. Partner nations that take achieving WPS objectives seriously probably also take supporting and protecting human rights seriously. In addition, integrating women into security and overall gender equality has been linked to durable postconflict peacebuilding, societal stability, peaceful conflict resolution, and higher overall socioeconomic development.²⁹ For the United States, these outcomes translate to regional stability and security aligned with the Interim National Security Strategy Guidance objectives. Additionally, WPS objectives and better integration of women into security give the United States a comparative advantage over near-peer competitors. Through WPS objectives, the United States is seeking to build a security relationship with the whole of society, as opposed to near-peer competitors that seek to simply reinforce the status quo. Human rights and WPS objectives demonstrate a clear soft power advantage that the United States has in its approach to security cooperation; it seeks to invest in the people of a country as opposed to grooming leaders for transactional access to partner nations. Even in highly conservative societies, integrating WPS concepts into SC activities has the potential to enhance the relationship with the United States, build interoperability, and help set the stage for access.

U.S. Guidance on WPS

U.S. action to further WPS objectives predates 2017; however, the WPS Act

served as the catalyst for the formal integration of gender and gender-based criteria into SC activities. This act tasked the Department of State, Department of Defense, Department of Homeland Security, and any other department or agency specified by the President to develop a common strategy to fulfill the policy objectives outlined in the legislation as well as develop appropriate goals, benchmarks, and performance metrics to ensure accountability and effectiveness of plans to achieve policy outcomes outlined in the legislation. In June 2020, DOD released the WPS Strategic Framework and Implementation Plan (SFIP) to organize and outline its efforts to achieve the objectives in the 2019 U.S. Strategy on Women, Peace, and Security (WPS Strategy).

The SFIP outlines three major objectives: “to model and employ WPS principles, to promote partner nation women’s participation, and to promote protection of partner nation civilians.”³⁰ The SFIP applies to the entire DOD and will require it not only to coordinate internally and across agencies but also to develop a whole-of-society approach, entailing engagement with civil society. SC activities, when seeking to incorporate SFIP and WPS Strategy principles, should try to go beyond the obvious low-hanging fruit of ensuring gender diversity and inclusion among participants. Modeling behavior may be a good place to start with some partner nations, but it alone will not lead to durable progress toward WPS Strategy objectives. An October 23, 2020, Office of the Under Secretary of Defense for Policy guidance memorandum reinforces the importance of WPS principles by requiring DOD to apply them to “the development of its policies, plans, doctrine, training, education, operations, and exercises.”³¹ In addition, UN-mandated military and peacekeeping operations, in which partner nations may participate, will often include objectives and outcomes related to the WPS agenda and UNSCR 1325.³² It is to the benefit of both the United States and partner nations to integrate WPS objectives into SC activities, beginning with planning.

Integrating WPS objectives into SC activities can be a difficult task even under the best of circumstances; it is nearly impossible if there is no clear guidance on how to go about it. Many SC planners may seek guidance from doctrine; its role is to provide “useful guidance to military leaders” as well as a “shared conceptual framework” on how tasks are to be accomplished.³³ However, Jody Prescott cites a “U.S. military failure to consider gender as an operational factor.”³⁴ Using gender-neutral language in doctrine and other guidance is not a reflection of gender neutrality as much as it is of gender exclusion. Upon further assessment of U.S. joint civil affairs doctrine, Prescott concludes, “The lens through which the operational environment is analyzed is male, apparently based on the assumption that what is applicable to the men in a civilian population is equally applicable to the women.”³⁵ Even within the U.S. Services, the U.S. military’s gender-neutral approach has not had the intended consequences of achieving gender equality. Kyleanne Hunter writes that in Iraq, the “intersection of a deeply gendered conflict with gender-neutral standards resulted in unintended [negative] consequences” for force effectiveness.³⁶ In Iraq, female U.S. Servicemembers were brought in for a “uniquely gendered reason”: to interact with local Iraqi women in ways that male U.S. Servicemembers could not. If the female Servicemembers were doing a job men could not (that is, serve on Lioness teams), women were seen as invaluable. Once this gendered job task was not the focus of female military members, unit cohesion decreased, as many male Servicemembers believed women would not be able to “hack it,” and it became increasingly difficult for “men to understand and often accept the importance of women.”³⁷ This attitude has led to problems with the U.S. military’s ability to recruit and retain women, dampening the force multiplier effects of gender balancing. If gender-neutral language does not work domestically, why would doctrine writers expect gender-neutral doctrine to provide an adequate guide to military planning? Therefore, without integrating WPS objectives into



Lieutenant Vicky Nguyen, Gender, Peace, and Security advisor with Royal Australian Navy, presents during "Women and Security during Disaster" lecture at Palawan State University, during Pacific Partnership 2022, Puerto Princesa, Philippines, August 12, 2022 (U.S. Navy/Jacob Woitzel)

SC planning, joint doctrine cannot provide adequate guidance to planners.

In addition to guidance on how to integrate WPS objectives into current SC planning and activities, effective integration requires cultural knowledge beyond the traditional sources of information often relied on by SC planners. Incorporating cultural gender knowledge of a partner nation when conducting SC planning assessments is now a must. Demographic breakdown of partner-nation participants is good information to include, but integrating WPS principles in a meaningful manner requires more—specifically, an understanding of the second- and third-order effects of any planned activity on both men and women considering their roles in a partner nation's society. This goal

is better accomplished through gender mainstreaming. Following the strategy of gender mainstreaming will ensure that SC activities actively support WPS principles. And not only will this strategy enhance DOD progress toward achieving the WPS Strategy objectives, it also will enhance the overall effectiveness of SC programs by ensuring all segments of society see a benefit to maintaining a relationship with the United States. By mainstreaming gender during the planning process, the United States can ensure that tangible benefits of SC activities reach both men and women.

It is important to reinforce that gender mainstreaming is not the same as gender balancing. Gender mainstreaming requires more than just increasing the number of women in each activity;

it includes such efforts as developing an understanding of why the number of women is limited to begin with. Such an understanding requires an investigation into why women do or do not join the security sector and what impediments they face once there. Impediments can be both policy-based (that is, policies against women in combat roles) or due to traditional gender norms. In addition, does the partner nation have the capacity to absorb an influx of women? Are there barracks? How would uniforms be adjusted to accommodate physical differences between men and women? How robust is the sexual assault prevention program? What type of policies does the partner nation have regarding pregnancy and childbirth? Without serious considerations of these types of issues, any program focused on



Army Major General Jami Shawley, Commanding General of Combined Joint Task Force–Horn of Africa, conveys importance of including women in discussion of security during Women, Peace, and Security Conference, March 21, 2023, in Nairobi, Kenya (U.S. Air Force/Rachel L. VanZale)

gender balancing will fail in the long run. Getting women to join is one thing; getting them to stay is another.

In general, because globally men dominate the security sector, the tangible and intangible benefits of security sector assistance, whether it be security assistance or security cooperation, fall disproportionately on men.³⁸ This is not to say that achieving the public good of security only affects men, but through these programs, it is often men who are being trained, learning new skills, or having access to travel and educational opportunities. The United States has tried to ameliorate this situation by incorporating gender-based targets for participation in programs such as international military education and training,³⁹ but for various reasons, such targets are often not met.⁴⁰ The gender balancing approach is a good start, but a gender mainstreaming approach will ensure that these gender-based targets lead to lasting change.

Until gender mainstreaming occurs, the United States will continue to fail to meet gender-balancing targets over the short and long term. This is not to say that the United States should abandon these efforts. Although five out of the six countries that receive the most security sector assistance continue to have large gender gaps, countries in which the United States has prioritized gender inclusion have smaller security sector gender gaps than the United States.⁴¹ Finally, in countries that have to make choices between guns and butter, incorporating WPS principles into security sector activities will make the perceived benefits of these programs more widespread among the beneficiary partner nation's society. It could also make any planned U.S.-backed security cooperation activity beneficial to all segments of society, not just the military sector. Security cooperation activities can thus enhance overall acceptance of U.S.

actions and activities among the general population, further building U.S. soft power and access to the partner nation.

Reflections on Mainstreaming Gender

The first and most vital step in the integration of WPS into SC activities must be accomplished during the assessment—the first activity in SC planning. An initial assessment “provides an understanding of the context, conditions, partner capabilities, and requirements to inform security cooperation planning and implementation.”⁴² Initial assessments can be conducted by means of a variety of tools and methods. Common methods and tools used in initial assessments include strengths, weaknesses, opportunities, and threats (SWOT) analysis; political, military, economic, social, information, and infrastructure (PMESII) analysis; and diplomatic, informational, military, and economic (DIME) analysis. Integrating

WPS objectives should begin with assessments that mainstream gender through conducting a gender-based analysis that moves beyond simple demographic information to include a “lens that brings into focus the roles, resources, and responsibilities of women and men within the system under analysis.”⁴³

Generally, these assessments should be conducted with input from all stakeholders, to include the partner nation. Partner-nation stakeholder teams should trend toward gender balancing as a start. When women are included in assessments, definition of problems, causes, and solutions can go beyond “abstract do-gooding with minimal connection to the battles [women] are waging . . . in their own communities.”⁴⁴ Both SWOT and PMESII are flexible tools in which information vital to gender mainstreaming can be captured. Through these basic analyses, SC planners can understand what roles men and women play in the security forces, the government, or the ministry of defense, and how security issues affect men and women differently. The table presents a list of possible questions for inclusion in a PMESII analysis; however, its list is by no means exhaustive, and the type of information required is situation dependent. When possible, it is important to include sex-disaggregated data, which can provide important information on who benefits from what, how women are integrated into society, and how to best target SC activities for the purposes of

integrating women. Sex-disaggregated information should also be tracked, to be included in subsequent assessments.

Under U.S. law, SC planners must consider “gender perspectives”; this process requires assessments to move beyond simply depicting that, say, piracy or human trafficking is an issue into capturing how these threats to security affect men and women differently—which is the heart of what it means to conduct a gender analysis. Providing this information can also make further assessments, such as determining what specific training and equipment a country would need to improve security, much clearer. For example, a state with weak borders may have difficulties with drug trafficking or human trafficking, and combating each of these requires different tactics, techniques, and procedures, thus affecting the type of SC activities needed for the United States to assist the state in developing capabilities. If interceptions include victims of sexual exploitation, a type of human trafficking that primarily affects women, security forces training needs to include how to process these types of victims. In addition, any recruitment activity associated with building this operational capacity may have to include gender-based representative milestones for effective implementation. A basic gender analysis can then be further enhanced through gender mainstreaming.

For example, if a significant SC initiative (SSCI) includes building capacity

to counter human trafficking, perhaps one of the activities would be to build a program to recruit and retain females to assist in processing the influx of female victims. Gender balancing would only direct SC planners toward increasing female presence in terms of numbers, possibly through the development of quotas. However, this will not be enough to retain female military members. Gender mainstreaming would demand an analysis as to why women are not joining in the first place, and if they join, why they are not staying. What are the formal and informal policies around female military members? Are all career fields open to them? Do women have a path of progression? And even if women do receive the training, are they allowed to practice in the field in which they were trained? Gender mainstreaming provides a tool to integrate gender perspectives to ensure meaningful progress is made toward achieving WPS objectives.

Requirements levied on SC planners through the assessment, monitoring, and evaluation (AM&E) framework should also consider a gender-based analysis. Depending on the results of the initial assessment, Office of the Under Secretary of Defense for Policy prioritization and planning processes, such as setting the SSCI objectives, should integrate WPS-informed goals in specific language whenever possible. When developing SSCI objectives, SC planners should be asking how the effects of the achievement

Table. Integrating Gendered Analysis Using PMESII

Dimension	Questions to Include
Political	What is the state of women's rights? How are they enforced? What is the political participation by gender? What political positions of power do women have? What role do women play in insurgencies? Are there female-based informal networks?
Military	What is the demographic breakdown of security forces? What positions do most women have within the MoD or other security agencies? What is the access to PME for men and women? Do security threats affect men and women differently?
Economic	What is the demographic breakdown of economic participation? What jobs do men and women generally hold? What type of production is associated with each gender? How are men and women affected by the economic situation of the country? How are the economic consumption needs of men and women different?
Social	What are the traditional gender roles in this society? Is there a shift in gender dynamics? Are there overlapping cleavages with gender identity? Who is educated? Is there a demographic difference in perception of U.S. involvement?
Information	Do men and women have equal access to information sources? Who is listened to? How do men and women generally communicate information?
Infrastructure	Who benefits from infrastructure? How do the infrastructure needs of men and women differ? How does the lack of infrastructure affect men and women? How does infrastructure insecurity affect men and women?



U.S. Army Master Sergeant Leia Puco, with U.S. Army Pacific Command, addresses Fijian government and civil society organization stakeholders at Fiji Women, Peace, and Security National Action Plan Orientation Workshop, in Suva, Fiji, September 20, 2022 (U.S. Army/Hailey Miller)

of the objective could fall on men and women within the partner-nation's society differently and adjust accordingly. It is important to remember that considering gender perspectives is not code for "woman" but a requirement to understand how programs may affect men and women differently.

For example, an NGO had an objective to decrease malnutrition rates for inhabitants of a refugee camp. Aid workers distributed sacks of raw bulgur wheat, and malnutrition rates for all groups except young men dropped. Single men were starving; many also died. When the NGO investigated why the starvation rate of young men was not decreasing, it found that they were eating the bulgur wheat raw. In its raw form, bulgur wheat has no nutritional value; it must be cooked. Because of traditional gender norms, single men did not know how to prepare bulgur wheat to eat; therefore,

they were starving to death "with the food that they needed in their hands."⁴⁵ How could this intervention have been different if the NGO had considered a gender perspective?

In addition, reforming SSCI objectives to be specific about what type of behavior the beneficiary partner nation should exhibit at the completion of the SSCI will provide a better basis to develop other AM&E products, such as the theory of change, the performance monitoring plan, and the five-year plan. Because SC planning is traditionally done "backward" (developing the objective and working down to activities needed), incorporating gender into SSCI objectives would also ensure that SC activities would be aligned with WPS outcomes at all levels. Additional steps should be taken to mainstream gender at all levels of the logic framework by asking at each level, "Who benefits?" when developing

and refining inputs, outputs, and outcomes. Looking at how men and women may benefit differently could also lead to important distinctions in performance indicator reference tools.

Especially at the input, output, and outcome levels, a gender-balancing approach (seeking to focus on ensuring greater gender representation) in addition to gender mainstreaming can yield more robust results and reportable data on progress being made toward achieving both the SSCI and WPS objectives.⁴⁶ Recruitment, education, training, exercises, key leader engagements, and institutional capacity-building activities should include gendered scenarios and gender-based milestones whenever possible. Including these milestones can also enhance performance monitoring by increasing the data available. For example, if an SSCI objective is to build maritime security, the working or transportation

habits of women and children greatly affected by maritime insecurity can become a proxy indicator of an increase or decrease in maritime security.

Gender-based milestones are a good start toward achieving WPS objectives, but they should be used together with gender mainstreaming at all levels of planning and execution. This method is integral to ameliorating some of the negative outcomes of integrating gender into SC activities. In male-dominated societies, women who join traditionally male careers (such as security forces) put themselves at great risk. In developing countries, joining security forces can be considered a “dangerous act” for women.⁴⁷ In partner nations where women constitute a larger percentage of security forces, institutions dealing with

sexual assault, gender discrimination, and mental and physical health support as well as physical support structures, such as women’s barracks, may need to be expanded and adequately resourced.⁴⁸

In addition, women who are recruited, regardless of their training, can often find themselves relegated to traditional roles, such as serving or cleaning, either due to lack of support or even to institutional barriers, such as the coding of combat positions as male-specific.⁴⁹ In such cases, institutional capacity-building initiatives may have to work closely with governments to recode positions as gender-neutral.⁵⁰ Ensuring security force institutions have proper infrastructure to support a greater number of women forces is an important defense institution-building issue, because provision

of these services is closely linked to force readiness and retention. Many women who were Afghanistan’s “firsts” (helicopter pilot, fixed-wing pilot) have fled the country and are now living in exile, fearing for their safety if they were to return.⁵¹ SC activities that seek to increase recruitment and retention of women need to assess the capacity of institutions to absorb the higher numbers.

Overcoming WPS Integration Obstacles

Some may argue that it is already difficult enough to develop and administer a program building a capability a partner nation desires; it can be next to impossible to integrate WPS objectives into security cooperation. For example, a recent update on barriers



Colonel Pam Ellison with Hawaii Army National Guard speaks to students on Women, Peace, and Security initiatives and integration into peacekeeping operations, in Pusat Misi Pemeliharaan, Indonesia, July 19, 2022 (U.S. Marine Corps/John Hall)

to the successful implementation of SC programs in Georgia cited cultural differences as a factor. A U.S. foreign area officer stated that “cultural gaps are typically a greater impediment to mutual understanding.”⁵² Georgia does have a history of relative gender equality; therefore, integrating WPS objectives should pose few additional obstacles.⁵³ However, countries that do not have a history or culture of gender equality may chafe at the paternalistic way another requirement is levied on them.

Recent examples in Nepal demonstrate that progress, although painfully slow, is possible if WPS objectives are prioritized and integrated from the very beginning of the planning process.⁵⁴ Additionally, the United States has not levied these requirements alone; it is simply following through on objectives rooted in UN initiatives. Getting partner nation buy-in on the importance of achieving WPS objectives can be approached the same way an SC officer does for other SC activities: identifying how WPS objectives overlap with the objectives and values of the partner nation. Information gleaned from the initial assessment, especially if it contains gender-disaggregated data analysis, can be useful in this endeavor. In addition, many countries already have NAPs that can be used as starting points for getting them to take an active role in integrating WPS objectives into planned activities. Integrating WPS objectives should be presented as a tool for achieving national and regional security objectives, not as an obstacle to them.

A secondary caveat that may pose challenges to integration of WPS objectives is that SC officers and planners may believe they lack subject matter expertise in gender mainstreaming and/or a sufficient understanding of how best to go about integrating the objectives into SC activities. DOD policy has already prioritized the integration of WPS into education and training, and the Defense Security Cooperation Agency has employed WPS subject matter experts to assist in the task of integrating WPS objectives into higher SC planning

objectives. But these people are only a small portion of the SC workforce. Introduction to gender perspectives should be included in professional military education curriculum at all levels to expand knowledge of the WPS regime across American military forces, raising awareness of the positive outcomes to all types of military operations when gender perspectives are addressed. It would also allow GENADs or other gender leaders to spend less time explaining concepts or convincing a skeptical audience and more time progressing toward achieving WPS objectives. After all, if men are involved, then gender is already involved.

Final Remarks

The purpose of security cooperation is to develop relationships, build capacity, and ensure access to partner nations to achieve U.S. objectives. The achievement of this purpose is enhanced through a holistic application of WPS through gender mainstreaming. But the lack of guidance on this process and the use of gender-neutral language in doctrine foster the exclusion of gender analyses in the planning and implementation of SC activities. Failure to mainstream gender risks telling only half the story of a partner nation. Partnership assessments based on incomplete information can lead to less well-defined SSCI objectives, theories of change, and logic frameworks. Without well-defined plans, SSCIs are less likely to produce the strategic effects SC planners are seeking to accomplish. Additionally, SC plans that do not mainstream gender into their analysis will have greater difficulty integrating WPS objectives into SC activities and making meaningful progress toward achieving them. **JFQ**

Notes

¹ U.S. Code Title 10, *Armed Forces*, § 301, “Definitions,” December 22, 2022, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section301&num=0&edition=prelim#sourcecredit>.

² “DSCA Celebrates 50th Anniversary,” Defense Security Cooperation Agency, 2021, <https://www.dscamilitary.com/50th-anniversary>.

³ Angela O’Mahony et al., *Assessing, Monitoring, and Evaluating Army Security Cooperation* (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2165.html.

⁴ Angelic Young, “Toward a More Inclusive Approach to U.S. Security Assistance,” U.S. Civil Society Working Group on Women, Peace, and Security, April 2018, <https://www.usip.org/sites/default/files/10th-US-CSWG-April-25-2018-Policy-Brief.pdf>.

⁵ Valerie Norville, *The Role of Women in Global Security*, Special Report 264 (Washington, DC: United States Institute of Peace, January 2011), https://www.usip.org/sites/default/files/SR264-The_role_of_Women_in_Global_Security.pdf; Cynthia Enloe, *Bananas, Beaches, and Bases: Making Feminist Sense of International Politics* (Berkeley: University of California Press, 2014), 34.

⁶ Anne A. Witkowski, “Integrating Gender Perspectives Within the Department of Defense,” *PRISM* 6, no. 1 (2016), 35, <https://cco.ndu.edu/PRISM/PRISM-volume-6-no1/Article/685073/integrating-gender-perspectives-within-the-department-of-defense/>.

⁷ Robert Egnell, “Gender Perspectives and Military Effectiveness: Implementing UN-SCR 1325 and the National Action Plan on Women, Peace, and Security,” *PRISM* 6, no. 1 (2016), 72–89, <https://cco.ndu.edu/PRISM/PRISM-volume-6-no1/Article/685108/gender-perspectives-and-military-effectiveness-implementing-unsr-1325-and-the/>.

⁸ Kathleen Turner, “The Rise of Female Suicide Bombers,” *Counter Terrorist Trends and Analyses* 8, no. 3 (March 2016), 15–19, <http://www.jstor.org/stable/26351404>.

⁹ Marie O’Reilly, “Inclusive Security and Peaceful Societies: Exploring the Evidence,” *PRISM* 6, no. 1 (2016), 21–33, <https://cco.ndu.edu/PRISM/PRISM-volume-6-no1/Article/685037/inclusive-security-and-peaceful-societies-exploring-the-evidence/>.

¹⁰ Joachim Ottosson, “Women’s Patterns of Movement as Indicators of the Security Situation,” in *Whose Security? Practical Examples of Gender Perspectives in Military Operations, 2015*, ed. Li Hammar and Annika Berg (Stockholm: Nordic Centre for Gender in Military Operations, February 2015), 32–33, https://issat.dcaf.ch/download/93672/1643012/whose_security_2015_Nordic_Centre_web_version.pdf.

¹¹ Egnell, “Gender Perspectives and Military Effectiveness,” 77.

¹² “Soldiers Not Numbers: Integrating Women Into African Militaries Must Go Beyond Quotas and Traditional Roles,” *African Defense Forum*, January 14, 2015, <https://adf-magazine.com/2015/01/soldiers-not-numbers/>.

¹³ *National Security Strategy* (Washington, DC: The White House, October 2022), 18, <https://nssarchive.us/wp-content/uploads/2022/10/Biden-Harris-Administra->

tions-National-Security-Strategy-10.2022.pdf.

¹⁴ Jody Prescott, "Gender Blindness in U.S. Doctrine," *Parameters* 50, no. 4 (Winter 2020), 21–32, <https://press.armywarcollege.edu/parameters/vol50/iss4/4>.

¹⁵ Tourunn L. Tryggstad, "Trick or Treat? The UN and Implementation of Security Council Resolution 1325 on Women, Peace, and Security," *Global Governance* 15, no. 4 (October–December 2009), 539–557.

¹⁶ United Nations Security Council Resolution (UNSCR) 1325 on Women, Peace, and Security, S/Res/1325, October 31, 2000, 4, https://peacemaker.un.org/sites/peacemaker.un.org/files/SC_ResolutionWomenPeaceSecurity_SRES1325%282000%29%28english_0.pdf.

¹⁷ Ibid., 2.

¹⁸ This context uses Stephen Krasner's definition of a *regime* as "principles, norms, rules, and decision-making procedures around which actor expectations converge in a given area." In this case, the given area is integration of UNSCR 1325. See Stephen D. Krasner, "Structural Causes of Regime Consequences: Regimes as Intervening Variables," *International Organizations* 36, no. 2 (Spring 1982), 182–205.

¹⁹ Paul Kirby and Laura J. Shepherd, "The Futures Past of the Women, Peace, and Security Agenda," *International Affairs* 92, no. 2 (2016), 373–392, <https://www.chatham-house.org/sites/default/files/publications/ia/inta92-2-08-shepherdkirby.pdf>.

²⁰ Ibid.

²¹ "Gender Mainstreaming," United Nations Entity for Gender Inequality and the Empowerment of Women, <https://www.un.org/womenwatch/osagi/gendermainstreaming.htm>.

²² *United States Strategy on Women, Peace, and Security* (Washington, DC: The White House, June 2019), 2, https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/06/WPS_Strategy_10_October2019.pdf.

²³ *National Defense Authorization Act for Fiscal Year 2020*, Pub. Law 116-92, 116th Cong., 1st sess., December 20, 2019.

²⁴ Ibid.

²⁵ "DOD Announces Women Peace and Security 2022 Report," Department of Defense (DOD), July 19, 2022, <https://www.defense.gov/News/Releases/Release/Article/3098291/dod-announces-women-peace-and-security-2022-report/source/dod-announces-women-peace-and-security-2022-report/>.

²⁶ Prescott, "Gender Blindness in U.S. Doctrine."

²⁷ Sophia Jones, "The Many Dangers of Being an Afghan Woman in Uniform," *New York Times*, October 5, 2018, <https://www.nytimes.com/2018/10/05/magazine/afghanistan-women-security-forces.html>.

²⁸ Interview conducted in June 2022.

²⁹ Åsa Ekvall, "Norms on Gender Equality and Violent Conflict," *E-International Rela-*

tions, June 10, 2013, <https://www.e-ir.info/pdf/39107>; Valerie M. Hudson, Donna Lee Bowen, and Perpetua Lynne Nielsen, "We Are Not Helpless: Addressing Structural Gender Inequality in Post-Conflict Societies," *PRISM* 6, no. 1 (2016), 122–139, <https://cco.ndu.edu/News/Article/685045/we-are-not-helpless-addressing-structural-gender-inequality-in-post-conflict-so/>.

³⁰ *Women, Peace, and Security Strategic Framework and Implementation Plan* (Washington, DC: DOD, June 2020), 10, <https://media.defense.gov/2020/jun/11/2002314428/-1/-1/1/women-peace-security-strategic-framework-implementation-plan.pdf>.

³¹ Office of the Under Secretary of Defense for Policy Memorandum, *Implementation of the Department's Women, Peace, and Security Strategic Initiative Framework and Implementation Plan* (Washington, DC: DOD, October 23, 2020).

³² Lena P. Kvarving and Rachel Grimes, "Why and How Gender Is Vital to Military Operations," in *Teaching Gender in the Military: A Handbook*, ed. Bojana Balon et al. (Geneva: Geneva Center for Democratic Control of the Armed Forces and Partnership for Peace Consortium, 2016), 9–25, <https://www.dcaf.ch/sites/default/files/publications/documents/DCAF-PfPC-Teaching-Gender-in-the-Military-Handbook.pdf>.

³³ Barry R. Posen, "Foreword: Military Doctrine and the Management of Uncertainty," *The Journal of Strategic Studies* 39, no. 2 (2016), 159–173, <https://www.tandfonline.com/doi/full/10.1080/01402390.2015.1115042>.

³⁴ Prescott, "Gender Blindness in U.S. Doctrine," 22.

³⁵ Ibid., 24.

³⁶ Kyleanne Hunter, "'In Iraq, We Were Never Neutral': Exploring the Effectiveness of 'Gender-Neutral' Standards in a Gendered War," *Journal of Veterans Studies* 7, no. 2 (2021), 8, <https://storage.googleapis.com/jnl-vt-j-jvs-files/journals/1/articles/265/submission/proof/265-1-1863-3-10-20210728.pdf>.

³⁷ Ibid., 7, 14, 15.

³⁸ Young, "Toward a More Inclusive Approach to U.S. Security Assistance."

³⁹ "International Training," in Defense Security Cooperation Assistance (DSCA) Manual 5105.38-M, *Security Assistance Management Manual* (Washington, DC: DSCA, 2012), <https://samm.dscs.mil/chapter/chapter-10#C10.6>.

⁴⁰ Jones, "The Many Dangers of Being an Afghan Woman in Uniform."

⁴¹ Ibid.

⁴² DOD Instruction 5132.14, *Assessment, Monitoring, and Evaluation Policy for the Security Cooperation Enterprise* (Washington, DC: DOD, January 2017), 13, https://open.defense.gov/portals/23/documents/foreignasst/dodi_513214_on_am&c.pdf.

⁴³ Quoted in Kathleen Staudt, "Gender Mainstreaming: Conceptual Links to Institutional Machineries," in *Mainstreaming Gender, Democratizing the State? Institutional Mechanisms for the Advancement of Women*, ed. Shirin M. Rai (Manchester, UK: Manchester University Press, 2003), 51, https://www.academia.edu/76640075/Gender_mainstreaming.

⁴⁴ Enloe, *Bananas, Beaches, and Bases*, 34.

⁴⁵ Sahar Alnouri, "Global Gender and Integration," video, 9:18, TEDx Portland Conference, 2012, <https://www.youtube.com/watch?v=2HCP1wAJyN4>.

⁴⁶ Egnell, "Gender Perspectives and Military Effectiveness."

⁴⁷ Jones, "The Many Dangers of Being an Afghan Woman in Uniform."

⁴⁸ Whitney Dudley and Robert Stewart, "Women in Special Security Forces: What the U.S. Can Learn From Afghans," *The Rand Blog*, March 28, 2016, <https://www.rand.org/blog/2016/03/women-in-special-forces-what-the-us-can-learn-from.html>.

⁴⁹ Jones, "The Many Dangers of Being an Afghan Woman in Uniform."

⁵⁰ Ibid.

⁵¹ Ibid.

⁵² Joseph C. Bilbo, brief to author, December 16, 2020.

⁵³ *Global Gender Gap Report 2020* (Geneva: World Economic Forum, 2020), https://www3.weforum.org/docs/WEF_GGGR_2020.pdf.

⁵⁴ Joe Evans and Akriti Rana, "Gender Considerations in Military Planning: Examples from Nepal," *Small Wars Journal*, February 4, 2018, <https://smallwarsjournal.com/jrnl/art/gender-considerations-military-planning-examples-nepal>.



Morgan Jungk, daughter of Master Sergeant Beth Jungk, 19th Communications Squadron plans and programs manager, has autism and other complex needs as she swings in her backyard on August 24, 2013, in Jacksonville, Arkansas (U.S. Air Force/Jake Barreiro)

The Exceptional Family Member Program

Noble Cause, Flawed System

By Benjamin T. Bryant

We recruit individuals, but we retain families.” This profound statement by a senior military leader during a conversation

Lieutenant Colonel Benjamin T. Bryant, USAF, is the Deputy Department Chair for Airpower in the Air Command and Staff College at Air University, Maxwell Air Force Base, Alabama.

at Air University in August 2021 astutely observes both the familial bonds that characterize the profession of arms and the challenge of maintaining those bonds while in the active defense of the Nation. The “we” is the Department of Defense (DOD), which appropriately frames the level of responsibility. Likewise, the “retain

families” mindset adroitly frames the scope of accountability.

The preeminent program whose purpose is to serve and care for the special needs of eligible families of Servicemembers is DOD’s Exceptional Family Member Program (EFMP). Concisely, the core of EFMP is the advocacy and facilitation of services to support

the needs of Servicemembers and their dependents who require more acute or specialized care than may be available at military base ecosystems, and EFMP's goal includes connecting people to these services. In execution, however, EFMP has foundational issues. For example, one military member commented that he and his spouse "wish that it wasn't such an arduous process to get her the required healthcare" and that communication of program processes was poor. Another military member commented that EFMP was central to their decades-long career and involved processes "that had too much bureaucracy in it."¹ To realize the scale of the impact that EFMP has on the force, realize that the first speaker is a staff sergeant, and the latter is the current Chief of Staff of the Air Force.

The strategic impact of such a program on the viability and sustainability of a military force and the families who support them is seminal. According to DOD's Fiscal Year (FY) 2020 EFMP report to Congress, an estimated 248,500 Active-duty Servicemembers and family members are enrolled in the program (roughly 9 percent of the force and dependents, not including Guard, Reserve, or DOD civilians).² That number is equivalent to every living person in either Orlando, FL, Pittsburgh, PA, Lincoln, NE, or Santa Ana, CA, being enrolled in the program, and this fact demands attention. Inarguably, this level of U.S. force projection capability affected by a singular program is strategically significant.

Accordingly, EFMP has congressional attention. As it has done with other serious issues plaguing the force, such as sexual assault and suicide prevention, Congress established improvement requirements for DOD and the military departments through its main resourcing tool, the National Defense Authorization Act (NDAA). The foundational obstacles plaguing the program arise from DOD's lack of centralized command, control, and communications, leading to nonstandardization, disparate program implementation and communication across the departments, uneven service availability at installations, and inefficient and ineffective insurance

processes. These foundational obstacles, in turn, have a cumulative effect on the Servicemember, which negatively affects DOD's collective human capital.

EFMP Nonstandardization

EFMP's lack of centralized command, control, and communications results in inconsistent standards, policies, practices, and services across DOD. The FY21 NDAA objectively addresses the issue of standardization within DOD, highlighting the disparately applied program across the departments.³ Specifically, the NDAA requires the Secretary of Defense, in coordination with the department secretaries, to standardize EFMP within 6 months of the enactment of the NDAA.⁴ Furthermore, the NDAA requires the Secretary of Defense to submit a standardization and implementation plan to the Armed Services Committees in the Senate and House of Representatives within 180 days of the enactment of the NDAA.⁵ Admittedly, this revelation of the non-standardization of EFMP is not revelatory at all. Neither the FY21 NDAA nor this article is the first to shed light on a foundational flaw in the program. For example, the Government Accountability Office (GAO) published a study in 2018 providing a critical finding that DOD had not standardized the program or had any measures by which to measure program efficacy.⁶ In 2020, GAO congressional testimony stated that DOD had yet to implement recommendations from the 2018 report.⁷ Furthermore, RAND's review in 2021 highlighted the significant level of differences in the program's application as a critical finding.⁸

Despite these studies, it is apparent that problems persist in the EFMP, requiring congressional oversight. As evidence of this issue, the FY20 DOD EFMP report to Congress in May 2021 listed standardization as the top priority in righting the ship, highlighting the efforts of DOD and the Services in doing so.⁹ While not arguing the efforts made, the results are noticeably absent. DOD's EFMP policy, as discussed below, is currently the guidepost for the

program. The reliance on this policy and subordinate departmental policies do not inspire confidence that the program is evenly distributed and applied. The 2018 GAO report on EFMP issues prompted Congress to act, as it has done in the past when the military has failed to address an issue.¹⁰ Four years have gone by since the GAO report with little to show in the way of standardization and efficacy improvements at the DOD level. So why did Congress address EFMP so decisively?

The congressional intent is clear: the accountability for developing and implementing a clear EFMP plan for the departments to implement rests with DOD. The manifestation of this centripetal requirement rests in a published and legally reviewed directive. Absent any unpublished updates, the most recent directive concerning EFMP at the DOD level is DOD Instruction (DODI) 1315.19, *The Exceptional Family Member Program*, dated June 23, 2023.¹¹ The document goes into detail as to the bureaucracy required to execute EFMP. However, it lacks the proper focus on the Servicemember and his or her dependents who require special needs by not explicitly opening the directive with *why* EFMP is so critical to the mission and the military family. While this tone is not in and of itself indicative of a directive written for the directive's sake, it does not inspire confidence that the program builds around the Servicemember and his or her dependent's needs. Finally, DODI places too much onus for program development, execution, and feedback on the departments. Specifically, the directive is more about reporting procedures and less about program purpose.¹² In this regard, the directive meets the intent of "up and out" congressional communication but not "down and in" leadership of the departments or facilitation for program beneficiaries. Failing to meet the design principle of form following function reveals itself in dated, unsynchronized, and non-integrated department regulations.

Uneven Service Availability

Not only does DOD's lack of centralized command, control, and communications engender disparate program

implementation and communications across the departments, it is also complicit in uneven service availability at installations. For example, the RAND EFMP study in 2021 highlighted a decided difference in services available to Servicemembers and their families from installation to installation.¹³ Service availability at the installation level has two facets that are illustrative: lack of services and the appearance of service availability when the reality is otherwise.

Lack of Services. A lack of service availability, or cumbersome access to care, is an issue that plagues EFMP. Additionally, it speaks to a lack of personnel in the military to provide EFMP services at the installation level, further straining a lack of resources outside the installation. Both indicate a capacity and capability gap, severely affecting the Servicemember and family.

In response to congressional requirements as listed in the FY17 and FY20 NDAA's, DOD announced the planned reduction of 12,801 medical billets across all departments to transition these positions to operational needs.¹⁴ One-third of these reductions would be absorbed by personnel in addition to their current duties or by not training students for attritional purposes, with the remaining two-thirds being adjudicated by other means.¹⁵ DOD's report maintains one crucial concern: medical care is nonnegotiable, and the reductions in military medical positions must be covered elsewhere, primarily by off-base providers.¹⁶ Of the 122 medical community networks evaluated by DOD, as a determinant in the reduction study, 68 networks were identified as "high risk" or "extreme risk" in absorbing additional workloads, meaning major impacts would occur or the network was incapable of supporting additional stress.¹⁷ While the reduction of military medical staff will affect all beneficiaries, EFMP families will face compounding issues due to a lack of specialty care both on and off base, either restricting assignment availability or sending families to a location where the community healthcare system is overly strained. An inadequately resourced care team for EFMP beneficiaries shifts the

burden to the community, imposing an additional hurdle to quality care and creating the appearance of services when the facts on the ground are quite different.

Appearance of Service Availability.

The appearance of, but not actual, service availability at a particular location arrests a Servicemember's and his or her family's critical care. One area of concern is medical capability and capacity. As DOD expands the requirements for an off-installation provider to be considered "trusted and accountable," a program the FY23 NDAA seeks to proliferate further to "shift risk from the DOD to civilian healthcare providers," the capability issue may resolve itself, but capacity is sure to be decremented.¹⁸ The risk may prove too heavy a burden for off-base providers to shoulder.

Another area of concern is public education capability and capacity, specifically special education related to EFMP. A 2019 Army survey and a 2010 Marine Corps survey shed light on the problems their respective EFMP families face in terms of transitioning special education services during an assignment change or ensuring that services are supported by the school system.¹⁹ Furthermore, in testimony to Congress in 2020, advocates conveyed Servicemembers' ordeals in dealing with both inadequate access to health care and inadequate support to individual education plans.²⁰ Far from localized either geographically or organizationally, the vignettes represented each Service and each region of the country.²¹ As the burden shifts to communities to support services such as health care and education, the strain on EFMP families increases, as many networks are ill equipped to fill the gap.

Worrisome Insurance Processes

TRICARE is the Defense Health Agency (DHA)-managed healthcare program charged with serving DOD Servicemembers, dependents, and retirees. TRICARE suffers from one major ineffective procedure and one significant inefficient process in executing this charge specific to those requiring specialized care through EFMP.

Insurance Ineffectiveness. In terms of ineffectiveness, one procedure bedevils TRICARE and causes inordinate harm to Servicemembers and their dependents: the curtailment of services, specifically the Autism Care Demonstration (ACD). According to TRICARE's Web site, ACD began in 2014, is authorized to operate through 2023, and covers Applied Behavior Analysis (ABA) services meant to target core symptoms of autism spectrum disorder (ASD).²² In 2020, the Assistant Secretary of Defense for Health Affairs (ASDHA) directed the Defense Health Board (DHB) to provide recommendations in modernizing TRICARE to position the program as a values-based healthcare provider.²³ The recommendations from the working group were unanimously accepted by the DHB and presented to the ASDHA in November 2020.²⁴ A consequential recommendation is that the nexus of care should revolve around an Accountable Care Organization (ACO).²⁵

Regarding autism and ABA, the recommendation is that TRICARE should evaluate ACOs based on outcome and precise patient-reported outcomes and ensure that providers have processes in place to care for complex conditions such as autism.²⁶ The result of such recommendations is a constriction of available providers and services based on the stricter rules governing TRICARE coverage. In early 2021, TRICARE released the changes to the ACD. Of note, there are no longer authorizations for Registered Behavior Technicians (RBT) in the school setting, and the authorization for ABA services is more restrictive than in the past.²⁷

The appearance of non-objectivity in reaching these decisions is of concern. Congress agrees, and the FY22 NDAA contains a provision for an independent review of ACD to judge its efficacy and provide recommendations to the Secretary of Defense.²⁸ Representative Bill Posey (R-FL), a member of the Congressional Autism Caucus, echoed this in an October 2021 letter to Secretary of Defense Lloyd J. Austin III urging an independent review of the ACD and rolling back the curtailments until an independent review is completed.²⁹



Kayleigh Norton, applied behavior analysis therapist, reviews numbers with Carl, son of Sarah and Technical Sergeant Carl Sole, 628th Security Forces Squadron flight chief, April 13, 2012, Joint Base Charleston, South Carolina (U.S. Air Force/Dennis Sloan)

Insurance Inefficiency. One inefficient process plagues TRICARE and causes inordinate harm to Servicemembers and their dependents: the requirement for Servicemembers and their families changing assignments across TRICARE regional boundaries to re-complete the referral process for services. Admittedly, this requirement is not the sole province of EFMP families; however, while all military families experience referral issues on an assignment change, EFMP families experience compounding issues due to a break in specialty services. Fortunately, the FY23 NDAA contains

language requiring DOD to report the impediments to removing this requirement.³⁰ One such impediment will be the lesser known link between TRICARE and Medicaid. EFMP beneficiaries, if they qualify, are often dependent on Medicaid to supplement healthcare costs when TRICARE will not cover the expense.³¹ Unfortunately, Medicaid benefits vary from state to state, meaning that what Medicaid might cover for an EFMP family in one state might not be covered in another.³² Out-of-pocket costs to EFMP families are an additional stressor in an already fraught scenario.

Impact on People

The strategic significance of the issues negatively affecting EFMP is palpable, specifically the effect these issues have on a sizable portion of the Nation's combat capability as it affects Servicemembers and their families. For example, according to a 2019 Army-sponsored survey of EFMP families, half of the respondents indicated they did not receive information about the program.³³ Additionally, the same percentage of respondents reported experiencing moderate, heavy, or severe impacts due to a military move, with



Child pets horse at Horses Help, April 20, 2019, in Phoenix, Arizona, as part of Luke Air Force Base's Exceptional Family Member Program (U.S. Air Force/Leala Marquez)

the percentage increasing for those with multiple moves.³⁴ Last, one-third of the respondents reported not receiving services at the gaining installation in addition to experiencing service unavailability or barriers to service.³⁵

According to a 2020 survey conducted by Partners in Promise, a nonprofit organization advocating for EFMP families, 40 percent of respondents were unfamiliar with the process, and 20 percent did not enroll for fear of negative impacts to career progression.³⁶ Moreover, 40 percent of respondents with EFMP students experienced issues, such as Individualized Education Program implementation, and 79 percent reported going more than a month at the new installation without receiving services.³⁷ According to a 2021 Partners in Promise survey, 39

percent of respondents reported going without special education services for their children after a military move, with an average wait time of nearly 6 months before receiving support.³⁸ While only 20 percent of respondents reported filing a claim due to a lack of legally required support, 74 percent reported the desire to do so.³⁹ Of note, this most recent survey found no delineation between the Services according to beneficiary experience.⁴⁰

According to a 2010 Marine Corps-sponsored survey, respondents noted challenges in accessing care, paying out of pocket, restrictive coverage, insurance processes, and teaming with the local school system, likening the preceding issues to “a continual struggle for parents.”⁴¹ The Navy (2020) and Air Force (2016) each surveyed their respective

forces, ostensibly with similar findings regarding EFMP inadequacies, based on congressional testimony.⁴² EFMP is a DOD responsibility and a community imperative to fulfill both Navy and Air Force mandates to the EFMP beneficiaries. However, the program has benefited from the attention of key stakeholders.

Senior Leader Perspective. General Charles Q. Brown, Jr., is the current Air Force Chief of Staff, and he and his wife, Mrs. Sharene Brown, are an EFMP family. During an interview to follow up on the Browns' Air Force Association Air, Space, and Cyber Conference Town Hall, they shared why they care so deeply about EFMP, where the program is currently, where it needs to be, how the military has improved, and how it should improve to close the gap.⁴³ The Browns have dealt with

EFMP throughout their time in service. As parents to a son diagnosed with autism, they have navigated the system as many military families have had to do, with both positive and not-so-positive experiences.⁴⁴ As “regular people” with life experiences and struggles relatable to EFMP families across the force, the Browns have been able to combine a passion for program improvement with a position by which to advocate for beneficiaries strategically.⁴⁵ General Brown also agrees that there should be increased national awareness concerning diagnoses such as autism and mental health needs, providing a fertile ground that furthers EFMP’s efficacy.⁴⁶ National awareness has spurred tremendous support through nonprofit organizations and local agencies to support EFMP needs. However, Mrs. Brown identified a need to synchronize and integrate

these virtuous yet disparate efforts into streamlined care.⁴⁷ She also offered that a troubling issue for EFMP was something that the military has been perennially poor at executing: marketing, especially when it comes to support programs internal to the military.⁴⁸ The Browns created and champion the Five and Thrive initiative, a program addressing top concerns of military families such as child care, education, health care, housing, and spouse employment.⁴⁹ Seminal to this initiative is active advertisement through multiple modes and mediums, creating local and national awareness.

The Browns see additional avenues for EFMP improvements, such as program standardization among the Services, program support for special needs adolescents transitioning into adulthood, feedback mechanisms to validate program

efficacy, and right-sizing resources in concert with TRICARE and DHA.⁵⁰ Moreover, the Browns discussed the need for the military community to speak in a “collective voice,” engendering advocacy at the highest government levels and continuing the momentum of EFMP improvement required to place the program among the pantheon of military-provided support viewed by beneficiaries as superlative to benefits provided by corporate America.⁵¹ Moving the needle in this direction is a crucial factor in retention. Through this keen insight and advocacy at the strategic level, EFMP now touts significant improvements.

Recent Success of Improvements

General Brown highlighted improvements that simplify, centralize, and standardize EFMP across the Air Force,



Shannon Scott, 325th Force Support Squadron Exceptional Family Member Program coordinator, talks to members of Tyndall community about special education resources on and off base at Tyndall Air Force Base, Florida, December 2, 2022 (U.S. Air Force/Zachary Nordheim)



Aircrew Survival Equipmentman 2nd Class Sonia Aquino, assigned to guided-missile destroyer USS *Gridley*, talks to child from Rehabilitation Institute for Autism during community service event in Manama, Bahrain, April 6, 2022 (U.S. Navy/Colby A. Mothershead)

and these efforts are led by the Air Force Personnel Center EFMP Central Cell.⁵² Since May 2020, the Central Cell has provided Servicemembers and their dependents with bimonthly updates on ongoing improvements, gaps yet to be addressed, and the plan moving forward. The updates include a Department of the Air Force Family Vector Web site that provides families access to plentiful EFMP resources any time and near-real-time information on what installations can and cannot support, as well as acceptance rates based on a specific condition or diagnosis.⁵³ Additionally, the updates include staff additions at the Central Cell, including a specialized attorney, a special education specialist, four regis-

tered nurses, a health benefits analyst, a respite care liaison, and a plan to hire four physicians soon.⁵⁴ Last, an update was made to the assignment change procedure, fully automating the Family Member Travel Screening process with no requirements for medical appointments and providing an entirely online experience for submitting forms and documents throughout the assignment process.⁵⁵ This update is ubiquitous in its usefulness to Servicemembers and their dependents. It promises to drastically reduce time and effort in navigating the change of assignment consideration process: acceptance or denial, appeal, and completion. The Army, Marine Corps, and Navy have likewise launched similar initiatives aimed at

facilitating “smooth moves” and services for their EFMP families. That said, General Brown acknowledges the challenges of nascent processes endeavoring to accomplish a complex mission.⁵⁶ However, given the organizational learning of the past year, he is confident that the teams facilitating EFMP improvement are on the right track in terms of capacity and capability to provide sustainable, repeatable, and timely support to EFMP families.⁵⁷

Recommendations

In addition to the possibility of scaling EFMP improvements across the force, there are effective ways to continue to steer the program in the spirit of its noble cause.

First, DOD must codify, coordinate, and communicate a comprehensive EFMP policy. An effective strategy for implementing EFMP at the DOD level prioritizes specialized care for beneficiaries in a principled way by matching actions with words. A coherent strategy signals to Congress how resources will be allocated to implement congressional mandates and gaps between current funding and required funding. A clear strategy communicates to beneficiaries what to expect from EFMP. An articulate strategy provides each department with the necessary details to develop their respective policies and the mechanisms to adjudicate program implementation issues. Currently, DOD's Office of Special Needs (OSN) and the Services are in the process of standardizing EFMP, which is a crucial first step, but it is certainly not the desired endstate. An active strategic narrative to market the program is essential to the success of a standardized program. OSN and the Services should consider writing EFMP regulations with the beneficiary in mind rather than the bureaucracy. Building trust with special needs families begins with a communications strategy that seeks shared understanding and creates a sense of appreciation by the beneficiary that program administration places them at the nexus of care. Information is the new key terrain and decisive point in any current environment. EFMP is no different. Akin to an application developer, there must be a collective mindset that EFMP is iterative and attuned to customer requirements at the speed of need.

Second, the Services should emulate and supplement the DOD Advisory Panel described in the House-approved version of the FY22 NDAA.⁵⁸ The President's signed version includes a requirement for DOD to establish an advisory panel comprising stakeholders in the leadership, administrative, and, most important, beneficiary realms of EFMP.⁵⁹ While this provision is a significant step forward in highlighting, devising, and recommending program updates to OSN for implementation across the departments, the House-approved version contains much more substance. In it, the Service

Vice Chiefs of Staff nominate the panel members, and members must represent the force's diversity and serve a 2-year term, except for one member who serves for 3 years.⁶⁰ These stipulations help to ensure that a broader range of perspectives, experiences, and proposed solutions are presented by an inclusive team to OSN for consideration. In addition, the term limit ensures that new perspectives are considered, and the 3-year term for one member establishes a process of continuity from term to term. This type of council at the Service level could put a more refined take on the Service-specific issues facing special needs families, function as conduits up and down levels of command, and better inform the DOD Advisory Council.

Third, DOD must make entry into the Services more attractive for trained providers in fields such as, but not limited to, pediatrics, mental health, and counseling. Generalists cover gaps in care, but this does not correlate to an even exchange of expertise. Along with a fully staffed EFMP office, military providers trained in the fields of medicine of greatest need for special needs families allow for a superb quality of service and quality of life and provide the departments greater flexibility in personnel moves. This buoyed staffing would better support all Servicemembers, not just those with special needs. For example, the Department of the Air Force launched a Developmental and Behavioral Health Family Readiness Center pilot program in 2020 to address this provider shortfall.⁶¹ In essence, the program sought to provide a "hub and spoke" model of care to small or remote locations that do not have adequate services.⁶² Through teleconsultation, virtual health, and provider travel, the department looks to address inefficient and ineffective care at some locations that affect EFMP services and personnel mobility.⁶³ The pilot program has shown positive results at two locations, and the plan is to resource and scale the program across the department.⁶⁴ While this program tempers the symptoms—and DOD should look at projecting a similar model across the Services—it does not cure the lack of

qualified providers in the Air Force. In addition to qualitative measures, Congress and DOD should refrain from reducing medical billets pending a review of the effects such reductions will cause to the Military Health System. While there may be efficiencies gained by reducing overhead and combining efforts, quantity has a value all its own. Given no decrease in demand, quantitative measures are critically important.

Fourth, DOD must engage with civic leaders who partner with the installation to broaden and deepen the services provided in the community, specifically in the fields of medicine, therapy, and education. For special needs families who desire the use of, or must use, off-base services for various reasons (including insurance necessity), a range of options to support special needs requirements enhances the installation and its mission. This synergy affords the departments greater flexibility in managing the force through assignment changes. Furthermore, it provides Servicemembers and their dependents peace of mind during the stressful assignment change process. This provides a linking mechanism between the installation and the community, furthering the cohesion of a critical civil-military relationship. One example of partnership is the DOD pilot program for allowing off-base military dependents to access education on base (currently reserved for on-base residents) to shore up lacking services in an area. As military medical positions are reduced, synergistic efforts between the installation and the surrounding community are crucial.

Fifth, DHA must allow Servicemembers and their dependents to transfer active referrals across TRICARE boundaries prior to, not after, permanently changing assignments to a new TRICARE region. This flexibility would remove the cumbersome process of starting the referral process again at a new installation. Furthermore, it removes costly wait times, which preclude critical special needs care for Servicemembers and their dependents when they could have been added to a waitlist while at their previous duty location. Referrals

for ABA already accomplish this through the Environmental Influences on Child Health Outcomes program, but other special needs services have long wait times, which could be minimized. At a new installation in a new TRICARE region, the primary care manager should not need to see the patient to aid in the referral transition process. The whole point of EFMP is to ascertain capability and capacity of care at the new installation. Once the change of assignment order is in hand, the Servicemember should be able to move referrals across TRICARE borders while also using services under that referral at the present location. The ability to remove arbitrary borders and the bureaucracy that comes with it substantially and more seamlessly enhances the continuation of care.

Sixth, DOD should roll back the curtailment of ABA services and exclusion of RBTs in the school setting. The FY22 NDAA contains a provision requiring an independent review of the efficacy of DOD's ACD program and ABA services.⁶⁵ While autism is just a subset of EFMP, it is a microcosm of the issues beleaguering the program—more precisely, the impression that EFMP is limiting services to or making the process more laborious for the most vulnerable population. An independent review might arrive at the same conclusion as DHA, but it might not. Nevertheless, an independent review would lend credibility and legitimacy to a decision that drastically affects Servicemembers and their families who depend on ABA services.

Lastly, DOD, much like it does regarding innovation efforts across the departments, should formulate a sustainable, repeatable, and measurable process for capturing best EFMP practices from across the force and push these to all Services for review and implementation as appropriate. As the sage advice posits, “Many hands make light work.”

Conclusion

The preceding recommendations are not all-encompassing, nor is the goal to perfect the program sensible. However, improvement is a realistic goal. The 2018 National Defense Strategy codifies

the importance of the men and women who serve in the Armed Forces either in uniform or in a civilian capacity by saying the “talent of the American warfighter is our greatest enduring strength, and one we do not take for granted.”⁶⁶ Unfortunately, the Cultivate Workforce Talent section does not mention the criticality of supporting Servicemembers or their families through initiatives such as EFMP.⁶⁷ Much like DOD policy regarding EFMP and the trickledown effect on Service-specific EFMP guidance, the lack of specificity on how DOD prioritizes quality of life calls into question the “not taken for granted” approach while also not setting the standard and expectation for the departments.

Engaged senior leaders such as General Brown, who laid out his people-first vision in his Chief of Staff of the Air Force Action Orders, are critical to creating a principled plan of action for improving EFMP.⁶⁸ As Simon Sinek offers, “For values or guiding principles to be truly effective, they have to be verbs . . . articulating our values as verbs gives us a clear idea.”⁶⁹

However, the program falls short of its guiding principle of Servicemember and dependent-centered special needs care. Suppose people are indeed DOD's competitive advantage. In that case, the strategic imperative of ensuring the support systems meant to care for Servicemembers and their families demands that EFMP does not exist as a bureaucracy solely for the bureaucracy's sake and that it is the most responsive, agile, and relevant program feasible. Providing sustainable resources of qualitative and quantitative substance will always be DOD's and the Services' sacred charge in caring for the military community.

Increasing the efficacy of the program is the right thing to do. It is also a prudent thing to do. The past three administrations have posited a world in which the character of war will shift in various degrees, one of which portends the return to a global struggle with peer competitors. While nonhuman resources, such as next-generation weaponry and cutting-edge Joint All-Domain Command and Control capabilities, capture the headlines, people

will be the deciding factor in the next conflict. EFMP is a strategic fulcrum with retention or separation hanging in the balance. As a strategic interest, EFMP is complex and requires deliberate development and resources over the next decade to produce lasting effects, capability, and capacity. Although complex, DOD cannot afford to lose talent due to the continued inadequacies of a program it administers. Therefore, EFMP must be a strategic priority as the geopolitical landscape shifts. Strategic competition with China and Russia requires it. Congress and its constituents demand it. Most important, the hundreds of thousands of Servicemembers and their families depending on EFMP, including my two sons diagnosed with autism, deserve it. **JFQ**

Notes

¹ Amanda Miller, “Caring for Their Son Gave the Browns a Window Into the Needs of Exceptional Families,” *Air and Space Forces Magazine*, September 27, 2021, <https://www.airforcemag.com/air-force-chief-of-staff-browns-son-autism-exceptional-families/>.

² *Annual Report to the Congressional Defense Committees on the Activities of the Office of Special Needs—2020, Pursuant to 10 U.S.C., § 1781c(b)* (Washington, DC: Department of Defense [DOD], May 2021), 5, <https://download.militaryonesource.mil/12038/MOS/Reports/osn-report-to-congress-2020.pdf>.

³ William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H. Res. 6395, 116th Cong., 2nd sess., *Congressional Record* 116, December 7, 2020, 652, <https://docs.house.gov/bills-s/20201207/CRPT-116hrpt617.pdf>.

⁴ *Ibid.*, 654.

⁵ *Ibid.*, 657.

⁶ Government Accountability Office (GAO), *Military Personnel: DOD Should Improve Its Oversight of the Exceptional Family Member Program*, GAO-18-348 (Washington, DC: GAO, May 8, 2018), <https://www.gao.gov/products/gao-18-348>.

⁷ GAO, *DOD Has Made Limited Progress Toward Improving Oversight of the Exceptional Family Member Program*, GAO-20-400T (Washington, DC: GAO, February 5, 2020), <https://www.gao.gov/products/gao-20-400t>.

⁸ Sarah O. Meadows et al., *The Exceptional Family Member Program (EFMP): Policy Alignment Between the Department of Defense and the Services* (Santa Monica, CA: RAND, 2021), https://www.rand.org/pubs/research_re-

ports/RRA742-1.html.

⁹ *Annual Report to the Congressional Defense Committees on the Activities of the Office of Special Needs*, 2.

¹⁰ William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 686.

¹¹ DOD Instruction 1315.19, *The Exceptional Family Member Program (EFMP)* (Washington, DC: DOD, June 23, 2023), 1, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/131519.pdf>.

¹² *Ibid.*, 6.

¹³ Meadows et al., *The Exceptional Family Member Program*.

¹⁴ *Report to the Congressional Armed Services Committees: Section 719 of the National Defense Authorization Act for Fiscal Year 2020*, Public Law 116-92 (Washington, DC: Under Secretary of Defense for Personnel and Readiness, July–August 2021), 1.

¹⁵ *Ibid.*, 2.

¹⁶ *Ibid.*, 28.

¹⁷ *Ibid.*, 30–31.

¹⁸ James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Public Law 117-70, 117th Cong., 2nd sess., December 6, 2022, 649–651, <https://www.congress.gov/bill/117th-congress/house-bill/7776/text>.

¹⁹ *Health of the Army Family: What We Know, What We Don't Know, and What's Next* (Washington, DC: Headquarters Department of the Army, December 2021), 67, <https://api.army.mil/e2/c/downloads/2022/06/15/04d8667e/haf-2021-report.pdf>; *United States Marine Corps Exceptional Family Members: How to Improve Access to Health Care, Special Education, and Long-Term Supports and Services for Family Members With Disabilities* (Washington, DC: National Council on Disability, November 2011), 3.1, <https://ncd.gov/publications/2011/Nov282011#toc40>.

²⁰ *Exceptional Family Member Program—Are the Military Services Really Taking Care of Business?* Hearing Before the Subcommittee on Military Personnel, House Armed Services Committee, 116th Cong., 2nd sess., February 5, 2020, 120–142, <https://www.govinfo.gov/content/pkg/CHRG-116hhrg43664/pdf/CHRG-116hhrg43664.pdf>.

²¹ *Ibid.*

²² “Autism Care Demonstration,” Plans and Eligibility, TRICARE, July 14, 2022, <https://tricare.mil/ACD>.

²³ *Modernization of the TRICARE Benefit* (Washington, DC: Defense Health Board, November 5, 2020), 3, <https://apps.dtic.mil/sti/pdfs/AD1116727.pdf>.

²⁴ *Ibid.*

²⁵ *Ibid.*, 25.

²⁶ *Ibid.*, 19.

²⁷ “Autism Care Demonstration.”

²⁸ National Defense Authorization Act for Fiscal Year 2022, Public Law 117-81, 117th

Cong., 1st sess., December 7, 2021, 634, <https://www.congress.gov/bill/117th-congress/senate-bill/1605/text/eah>.

²⁹ Representative Bill Posey (R-FL), letter to Secretary of Defense Lloyd J. Austin III, October 1, 2021, letter in author's possession.

³⁰ James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, 604.

³¹ “Medicaid for Family Members With Special Needs,” *Military OneSource*, March 22, 2022, <https://www.militaryonesource.mil/special-needs/medical-needs/medicaid-for-family-members-with-special-needs/>.

³² *Ibid.*

³³ Jill A. Brown et al., *Exceptional Family Member Program Survey: Assessing the Needs of Exceptional Army Families*, Public Health Assessment Report No. S.0065576-19 (Washington, DC: Headquarters Department of the Army, Health Promotion and Wellness, Public Health Assessment Division, July 2019), ii, <https://apps.dtic.mil/sti/pdfs/AD1095007.pdf>.

³⁴ *Ibid.*, 9.

³⁵ *Ibid.*, ii.

³⁶ Rebecca Alwine, “Survey Says Families Aren't Using EFMP Because They Don't Know How,” *Military.com*, February 2, 2021, <https://www.military.com/2021/02/02/survey-says-families-arent-using-efmp-because-they-dont-know-how.html>.

³⁷ *Ibid.*

³⁸ Karen Jowers, “Military Kids Face Delays, Inequities in Getting Special Education Services,” *Air Force Times*, February 3, 2022, <https://www.airforcetimes.com/pay-benefits/2022/02/03/military-kids-face-delays-in-equities-in-getting-special-education-services/>.

³⁹ *Ibid.*

⁴⁰ *Ibid.*

⁴¹ *United States Marine Corps Exceptional Family Members*, 3.1.

⁴² Amanda Dolasinski, “Navy Launches Survey to Hear From Special Needs Families,” Military Officers Association of America, June 3, 2020, <https://www.moaa.org/content/publications-and-media/news-articles/2020-news-articles/navy-launches-survey-to-hear-from-special-needs-families/>; “Exceptional Family Member Program—Are the Military Services Really Taking Care of Business?” 179.

⁴³ Miller, “Caring for Their Son Gave the Browns a Window Into the Needs of Exceptional Families.”

⁴⁴ General Charles Q. Brown, Jr., and Sharene Brown, interview by author, Washington, DC, March 2, 2022.

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

⁴⁷ *Ibid.*

⁴⁸ *Ibid.*

⁴⁹ *Ibid.*

⁵⁰ *Ibid.*

⁵¹ *Ibid.*

⁵² *Ibid.*

⁵³ Tammy Hern and Tami Nelson, “Update

on the EFMP Central Cell Special Education Program and Special Education Legal Services,” Facebook video, October 28, 2021, <https://m.facebook.com/AirForceEFMP>.

⁵⁴ *Ibid.*

⁵⁵ *Ibid.*

⁵⁶ Author interview with General and Mrs. Brown.

⁵⁷ *Ibid.*

⁵⁸ National Defense Authorization Act for Fiscal Year 2022, H. Res. 4350, 117th Cong., 1st sess., October 18, 2021, 530, <https://www.congress.gov/117/bills/hr4350/BILLS-117hr4350pcs.pdf>.

⁵⁹ National Defense Authorization Act for Fiscal Year 2022, December 7, 2021, 496.

⁶⁰ National Defense Authorization Act for Fiscal Year 2022, October 18, 2021, 532–533.

⁶¹ Colonel Kristine M. Hackett, “Talking Paper on Developmental and Behavioral Health Family Readiness Centers (DBFRCs),” Air Force Surgeon General email in author's possession, 2021, 1.

⁶² *Ibid.*

⁶³ *Ibid.*

⁶⁴ *Ibid.*

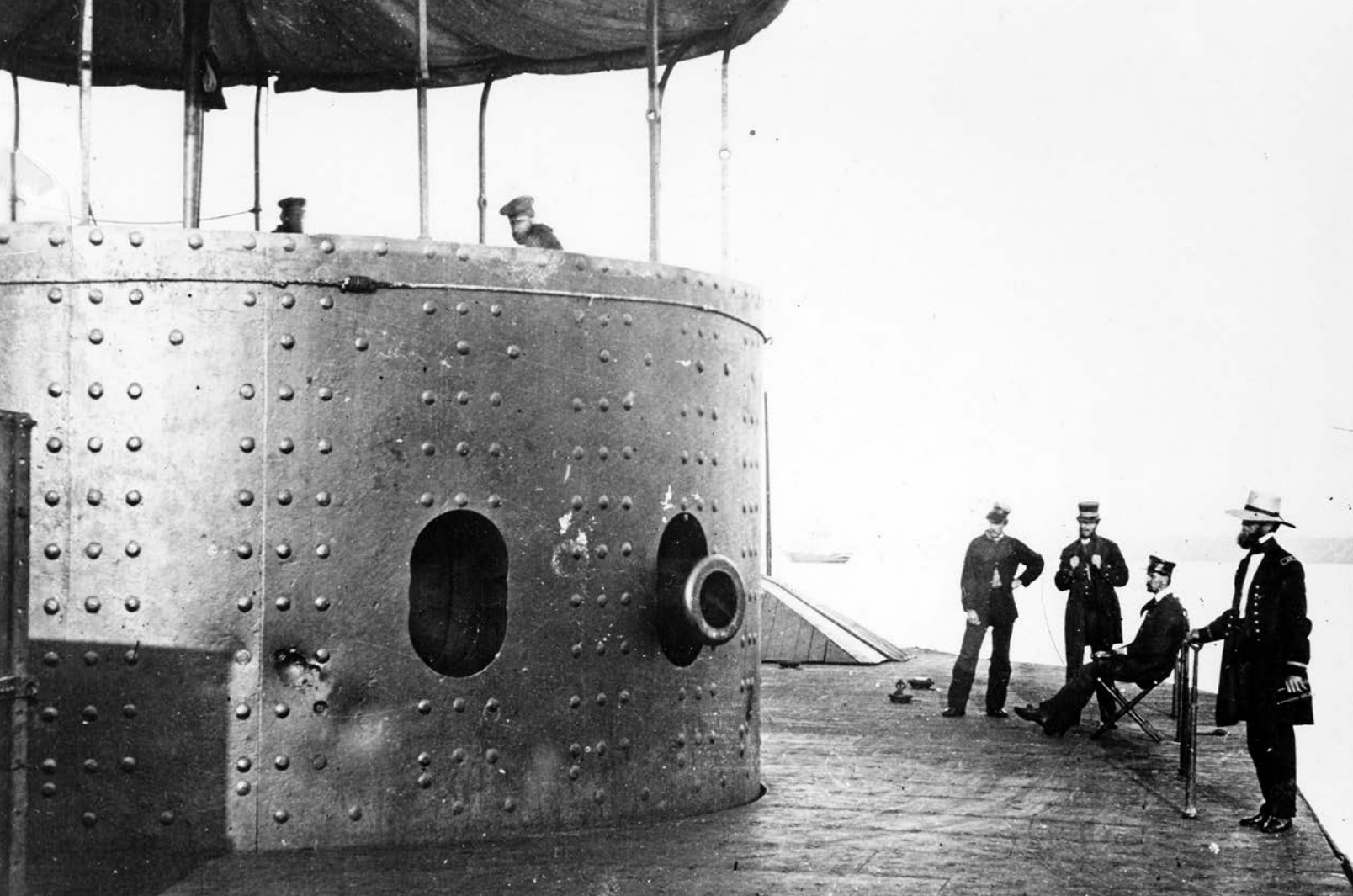
⁶⁵ National Defense Authorization Act for Fiscal Year 2022, December 7, 2021, 634.

⁶⁶ *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DOD, 2018), 8, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

⁶⁷ *Ibid.*, 7–8.

⁶⁸ General Charles Q. Brown, Jr., *CSAF Action Orders: To Accelerate Change Across the Air Force* (Washington, DC: Headquarters Department of the Air Force, 2020), 3, https://www.af.mil/Portals/1/documents/csaf/CSAF_Action_Orders_Letter_to_the_Force.pdf.

⁶⁹ Simon Sinek, *Start With Why: How Great Leaders Inspire Everyone to Take Action* (New York: Portfolio, 2009), 67.



Deck of USS *Monitor*, on James River in Virginia, July 9, 1862; officers at right (left to right): Third Assistant Engineer Robinson W. Hands, Acting Master Louis N. Stodder, Second Assistant Engineer Albert B. Campbell (seated), and Acting Volunteer Lieutenant William Flye (with binoculars) (U.S. Navy/Naval History and Heritage Command)

The Civil War and Revolutions in Naval Affairs

Lessons for Today

By David C. Gompert and Hans Binnendijk

At certain times, the character of naval warfare and the course of naval history undergo rapid, pro-

found, and lasting change. The American Civil War was such a time, and its lessons still resound.

David C. Gompert is on the faculty of the U.S. Naval Academy and is a senior advisor to Ultratech Capital Partners. He was Principal Deputy Director and Acting Director of National Intelligence, 2009–2010. Hans Binnendijk is a Distinguished Fellow at the Atlantic Council. He was previously NSC Senior Director for Defense Policy, Acting Director of the State Department Policy Planning Staff, and Director of the National Defense University's Institute for National Strategic Studies. Both authors are on the Board of Directors of the American Civil War Museum.

Because secession swiftly followed Abraham Lincoln's election to the U.S. Presidency, war came before either side was prepared. Both North and South scrambled to assemble available officers, Sailors, and ships. Soon, the inadequacies of off-the-shelf capabilities forced both sides to build better ones. Because the Union's naval strategy was more ambitious, and its technological and

industrial capacities more prodigious, it drove the Civil War's naval revolution. Yet the overmatched Confederacy would improvise tactics and weapons, some of them also revolutionary.

This revolution pivoted on the wholesale replacement of old warships with new ones. Prewar ships-of-the-line were wooden-hulled, wind-driven, and laden with large numbers of ineffective guns.¹ By war's end, warships were clad in metal, propelled by steam and screw, and armed with more accurate guns mounted in rotating turrets. They were more maneuverable, versatile, survivable, and lethal and were indifferent to currents and winds. They could operate on the high seas and in narrow inland waters. Within a year, Northern squadrons were pummeling Southern forts, conducting amphibious landings, transporting troops, and waging riverine warfare.

This revolution, like others, was the product of strategic need and emerging technology. The relationship between strategy and technology is fluid and complex. Strategy called for by looming threats presents demands that can be met by exploiting available or novel technologies. At the same time, exogenous technological change can excite unorthodox thinking about how best to execute strategy. Such "strategy-pull" and "technology-push" phenomena were both at play during the Civil War, as they are today.

An unanticipated danger—Southern secession—gave birth to a Northern strategy that called for new tasks as well as concepts of operations to perform them. These, in turn, demanded better capabilities—for example, steam-driven ironclads, made possible by concurrent technological advances. Northern industrial mobilization forged these new capabilities into a national capacity to fight across thousands of miles of water and shore. Along the way, it took bold and inventive leaders to steer the process and to employ forces in unprecedented ways.

These fundamental dynamics of the Civil War's revolution in naval affairs defined subsequent revolutions, and they pertain today.

The Union's Revolution in Naval Affairs

Union Strategy. The Anaconda Plan, put forward by Lieutenant General Winfield Scott in early 1861, was a strategy to strangle the seceding states by denying them trade through blockading saltwater ports and controlling the Mississippi River.² Scott's idea called for naval operations on two fronts. Union warships would blockade about 180 ports along some 3,500 miles of Confederate coastline. On the Mississippi, a force of around 60,000 Union troops, transported in 40 vessels and convoyed by 20 river gunboats, would steam downriver, capturing forts along the way until they reached New Orleans. They would then be reinforced by large army units to hold conquered territory as the flotilla patrolled the river. Should this naval strategy fail to reverse secession, Scott reasoned, Richmond would need to be taken.³

Initially, implementation of Anaconda was hampered by lack of suitable warships. It soon became clear that a much larger and better fleet would be needed to stop blockade-runners and thereby establish an "effective" blockade under international law. (An attempted but ineffective blockade could be legally ignored by foreign powers.) Also, the Union would need to seize Southern ports from which runners were operating and establish supply and coaling stations along the South's coasts to reduce steaming distances and time. As a stopgap measure, civilian vessels were hastily converted to warships.

The planned expedition down the Mississippi was deferred while Brigadier General Ulysses S. Grant and Flag Officer Andrew Foote fought their way up the Tennessee and Cumberland rivers for the purpose of controlling Kentucky and subduing Tennessee. Union victories at Fort Henry and Fort Donelson in February 1862 demonstrated the value of joint operations. Foote's flotilla then advanced down the Mississippi to defeat Confederate defenses at Island Number 10. Elements of the flotilla also supported Grant at the Battle of Shiloh, showing how naval fire could advantage land operations.

After Flag Officer David Farragut seized New Orleans in April 1862,

Union blue-water ships, both steam and sail, advanced up the Mississippi to meet the riverine flotilla coming down under Foote and, later, Commodore David Porter. But they were both halted beneath the fortress at Vicksburg, Mississippi, where Union ships were exposed to brutal fire. Because Vicksburg's being in Confederate hands prevented control of the Mississippi and encirclement of the South, the city became a Union preoccupation. Attempts to position Union troops to attack it by digging canals and clearing the Yazoo River of torpedoes (later called mines) were to no avail. Eventually, Porter's squadrons ran past Vicksburg's batteries and transported Grant's troops from the Western bank across the river south of the city.

Attacking Southern ports and forts proved far more efficacious than trying to intercept blockade-runners. On the Atlantic coast, Union victories in 1861 and 1862 at Port Royal, Roanoke Island, Hampton Roads, Fort Macon, and Fort Pulaski closed key Confederate harbors, leaving Charleston and Wilmington on the Atlantic and Mobile and Galveston on the Gulf of Mexico for the use of runners. Charleston was closed in 1863, Mobile in 1864, and Wilmington in 1865. Only Galveston remained under Confederate control when the war ended, by which time the Southern economy was moribund.

Emerging Tasks, Concepts of Operation, and Requirements. The tasks and associated concepts of operation required by Union strategy would inspire new uses of technologies to construct the capabilities they demanded.

Intercepting blockade-runners. Confederate blockade-runners initially had decided advantages. Blockaders had to cover the entire Southern coastline with limited numbers of seaworthy ships. Runners could choose opportune times and routes to make the 500- to 1,000-mile runs to the Bahamas, Bermuda, and Cuba. In the war's first year, a mere one out of ten runners was captured.⁴ To carry out the Anaconda strategy, the Union required more and faster ships and gunnery with greater range and accuracy to control the ports from which runners operated.

Defeating Confederate ironclads. At first, Confederate ironclads presented serious problems for Union operations in key waters—for example, CSS *Virginia* at Hampton Roads, CSS *Chicora* and CSS *Palmetto State* in Charleston Harbor, and CSS *Arkansas* near Vicksburg. Then, USS *Monitor*'s battle against CSS *Virginia* and subsequent ironclad duels demonstrated the advantages of speed, thick armor, a low profile, armor-piercing shells, accurate guns, rotating turrets, maneuverability, and ramming capability. Eventually, Confederate ironclads were either run aground (CSS *Atlanta*), destroyed in their harbors (CSS *Albemarle*), scuttled by the Confederates themselves to avoid capture (CSS *Tennessee* and CSS *Virginia*), or confined to British shipyards by U.S. diplomatic pressure.

Bombarding forts into submission. With Confederate forts impeding Union passage along the Mississippi and guarding major Southern seaports, the Union faced several new tasks. With steam-powered ships, the Union Navy improvised bombardment tactics whereby its gunships would steam continuously in oval patterns, thus becoming less vulnerable and optimizing firing angles. Also, ironclads could sail close to their targets to get off better shots. The operation against Georgia's Fort Pulaski in April 1862, led by the army, demonstrated for the first time the power of rifled artillery against previously indestructible walls.⁵

Bypassing Confederate forts. When Confederate forts were too hard to attack frontally from the water, Union ships were tasked to "run the gauntlet" through heavy fire to gain a better position from which to attack, as Farragut did at New Orleans. Such runs required speed, covering fire, and armor. Once they were completed, enemy forts often fell to siege and army-navy assault.

Supporting army operations with convoys, amphibious operations, and direct fires. Although there was no such thing as a formal joint army-navy command during the Civil War, victory often took army-navy cooperation.⁶ Grant and Foote partnered to take Fort Henry and Fort Donelson. Naval gunfire helped save Grant at Shiloh. Vicksburg finally fell

because Grant and Porter collaborated closely. Throughout the war, naval gunboats convoyed transports to bring troops to battle. At North Carolina's Fort Fisher, ships provided covering fire for advancing army troops.⁷

Destroying Confederate raiders. Early in the war, Jefferson Davis commissioned Confederate raiders, which captured and often burned hundreds of Union merchant ships. One of his aims was to force the Union Navy to detach large numbers of ships to go after privateers instead of performing blockade duties. Several fast ships were built for the Confederacy in England, including CSS *Alabama* and CSS *Florida*. Enraged Northern merchants pressured the Union Navy to catch raiders around the globe, which it did, with both sail and steam power.

Clearly, the Anaconda strategy would have failed without new warships. Riverine warfare required the maneuverability, lethality, and survivability that only steam-propelled armored ships could provide. These gunboats gained and kept control of the Mississippi, escorted convoys, and transported troops. During General Ambrose Burnside's Hatteras campaign, gunboats convoyed 12,000 troops in one day to seize the forts guarding New Bern, which fell thanks to bombardment by those same gunboats in support of those troops.⁸ Overall, the tasks and operational concepts necessitated by Union strategy transformed naval warfare for good.

Emerging Technology. These challenges summoned Northern inventiveness. There really is such a thing as "Yankee ingenuity." Finding technical solutions to practical problems came naturally in harsh, chilly, rocky New England, the epicenter of the American Industrial Revolution. The region's needs for both agricultural productivity and commercial competitiveness were answered by its inventiveness. Ivy League colleges and the Massachusetts Institute of Technology (founded in 1861) offered unmatched scientific educations. The Northeast gave the Union Navy some of its most creative leaders: Porter, Foote, Rear Admiral John Dahlgren, Navy Secretary Gideon Welles, and

Assistant Navy Secretary Gustavus Fox. Technology was already progressing rapidly in the North when the Civil War began, owing to a flurry of inventions. By the mid-19th century, the patent system had established the sanctity of intellectual property, making invention more rewarding than ever. The number of utility patents issued annually increased from 884 in 1850, 4,363 in 1860, and 12,157 in 1870, to 22,065 by 1897.⁹

The most important naval innovation was steam propulsion. In a typical system, fossil fuel (initially coal, later oil) was burned in a boiler to turn water into the pressurized steam needed to drive reciprocating pistons (later turbines) to rotate the ship's shaft and screw, and thus propel the ship.¹⁰ The steam was then converted back to liquid by intake of water, to be boiled again to keep the shaft turning. Screw revolutions per minute—thus ship's speed—were governed by varying steam force on the pistons.

The success of Union strategy also hinged on the use of metal-armored ships. Over millennia, since the Bronze and Iron ages, innovations in mining, extraction of metal from ore, smelting, shaping, and use of coal and coke put in place the means to produce the iron and steel that were used in the Industrial Revolution to make machines and infrastructure. Henry Bessemer is credited with inventing a high-volume steelmaking process 5 years before the American Civil War. Even then, iron was cheaper and easier to make than steel, the latter reserved primarily for small arms. Clad in iron, warships were largely invincible to the weapons of the time.

Innovation also improved gunnery. Technologies in this area advanced rapidly before and during the Civil War. Rifling of gun barrels with spiral grooves was invented centuries earlier, but weapons with this feature were first manufactured on a large scale in the 1850s. Rifling dramatically improved accuracy by spinning and stabilizing projectiles. Around the same time, John Dahlgren invented the "soda-bottle" smooth-bore cannon with a large chamber to increase explosive force and thus range and destructive force. Machined gun sights, percussion



USS *Monitor* crewmembers cooking on deck, on James River in Virginia, July 9, 1862 (U.S. Navy/Courtesy Ronnie Bell)

locks, and new methods for estimating ballistic trajectories improved accuracy, giving ships equipped with the new weapons an edge over shore fortifications.

Union Capabilities. The late Donald Rumsfeld's classic admonishment, "You go to war with the Army you have," describes both Union and Confederate predicaments in 1861. For the Union, "the Navy you have" consisted of a few old warships mostly powered by sail or paddlewheel, which proved unfit for the Anaconda strategy and demanded wholesale replacement.

No warship was more revolutionary than USS *Monitor*. Early on, Navy Secretary Welles commissioned John Ericsson, a renowned Swedish-born inventor, to build a ship capable of defeating any enemy ironclad. Although many technologies in *Monitor* had been experimented with before, they were now assembled in a radically new manner. The ship had just a foot of freeboard, making it hard to target,

and a heavily armored, stout, rotating turret with two of the best guns in service. Being nearly impregnable and packing considerable power, *Monitor* became the icon of Union warships.¹¹ Different monitors were developed for river, harbor, coastal, and seagoing missions, with more than 60 built during the war.

One consequence of the switch from sail to steam, as noted, was the shift of advantage from shore to shipboard gunnery. Steam provided a further edge over shore batteries by increasing ship speed and maneuverability. Striking a moving ship at significant distance was—and still is—extremely difficult. Examples abound of Union steam warships of several types successfully attacking and/or circumventing Confederate forts. Naval bombardment contributed significantly to victory in several cases, including Fort Hatteras and Fort Clark (Hatteras Inlet in August 1861), Fort Henry (Tennessee River in February 1862), Fort Jackson

and Fort St. Philip (New Orleans in April 1862), Fort Macon (Beaufort Harbor in April 1862), Fort Wagner (Charleston in April 1863), Fort Morgan (Mobile Bay in August 1864), and Fort Fisher (Wilmington in December 1864).

New warships facilitated joint army-navy operations, starting with Fort Donelson and extending during the war to all Southern coasts and riverbanks.¹² Joint operations encompassed coordinated land and water bombardment, amphibious landings, and softening up fortifications for troops to occupy.

Although the number of gunnery shells made for the Union fleet increased dramatically, rapidity of firing is a better metric of capacity. Breech loading was faster than muzzle loading. The average rate for all Union gunnery was between five and eight rounds per minute per barrel. Magazine elevators enabled nonstop, rapid, withering fire. Porter's fleet contributed 22,000



USS *Onondaga*, on James River in Virginia, ca. 1864–1865, with rowboat in foreground manned by Union Soldiers (Naval History and Heritage Command/Brady & Company)

projectiles to the defeat of Vicksburg.¹³ Dahlgren's fleet fired unrelentingly for two months on the Confederate fortifications on Morris Island guarding Charleston Harbor: USS *New Ironsides* alone fired 4,439 projectiles, and the accompanying monitors fired 3,577 more.¹⁴ Coupled with ground assaults, this bombardment eventually forced abandonment of Fort Wagner.

Industrial Mobilization. The Civil War's naval revolution was fed by two other revolutions:¹⁵ the French Revolution, which led to the Napoleonic political phenomenon of national mobilization, and the Industrial Revolution, begun with the advent of the steam

engine, which led to the mechanization of warfare on a vast scale. Together, these developments set the stage for unprecedented industrial mobilization in the North during the Civil War, which added heft to innovation.

As the North's ability to wage war grew, the evolving Anaconda strategy, General William Tecumseh Sherman's March to the Sea, and General Philip Sheridan's operations in the Shenandoah Valley combined to destroy the South's ability to wage war. Transportation came to a near halt; the South's railroads were in shambles, its major rivers under Union control. Southern destruction was in proportion to Northern mobilization.

The Confederacy got weaker as the Union got stronger.

This eventually yawning gap can be traced back to differences in size and makeup of the two economies. The North's industrial revolution powered huge increases in productivity. Nearly 90 percent of all U.S. industrial production resided in the North. The Union had 11 times the ships and 32 times the number of weapons manufacturers as the South. Meanwhile, the principal "productive" assets of the Southern economy were slaves and land. Because navies are capital-intensive, slavery diverted from the Confederacy's ability to wage war on the water.

Geography also influenced war-making capacity. The Erie Canal, completed in 1825, facilitated economic intercourse between the Northeast and the Northwest. This trade continued to grow as railroads replaced canals. Consequently, the North's capacity to make the machinery of war was integrated both vertically and transregionally. In contrast, the South's addiction to and investment in high-volume, high-margin cotton production, owing to the availability of enslaved labor, crowded out industrialization. Virginia, with relatively little cotton, was the only Confederate state with a modicum of industry, such as Richmond's famous Tredegar Iron Works (which relied in part on slave labor).

The need to accelerate mobilization came from the realization that the war would drag on and expand. The North had ample potential for industrial mobilization, owing to its growing population, agricultural self-sufficiency, preexisting manufacturing base (due to doubling of investment in manufacturing in the 1850s), and financial capacity (based on a growing banking system and revenue from California gold). At war, the North's industrial mobilization expanded as its economy grew by 20 percent from 1862 to 1864. By 1865, the Confederate economy was in ruins, with massive inflation and commerce reduced to bartering.

The bulk of Northern industrial mobilization consisted of the machinery of war: railroads and ships. Although the total number of Northern factories did not ramp up appreciably—the North already had 110,000 factories in 1861—production of iron and steamships did. When the war began, the North was producing 20 times more iron than the South.¹⁶ That and its greater capacity to produce steam engines led to the Union's preponderance of gunboats. When the war began, the Union had 42 commissioned ships, including sailing vessels of doubtful utility. By the end, it had 626 ships, including 84 ironclads carrying 4,610 guns. To 9,000 seamen in 1861, the Union Navy added another 50,000 during the war. By 1865, the Union Navy was the world's largest.¹⁷

Union Leadership. Senior Union naval officers typically excelled in battle, got the most out of their new capabilities and crews, and left lasting imprints on how war is waged on the water. Many were quick learners and unhesitant innovators, captives of neither tradition nor rigid career expectations. Farragut, Dahlgren, and Foote stood out in all these respects. Not far behind were Porter and Samuel Du Pont. Secretary of the Navy Gideon Welles and Assistant Secretary Gustavus Fox got high marks for vision, political savvy, and commitment to ensure that commanders got the capabilities they needed.

Exceptional leadership was critical during the Civil War for three reasons. First, the new war on water was unlike the previous experiences naval officers Farragut, Porter, and Du Pont had seen in action in the Mexican War, but the opposition they faced there was minimal. Moreover, the capabilities officers were given with which to fight—fast, armored steam warships with advanced gunnery—were unfamiliar. Nonetheless, a good number of senior Union naval officers not only adapted readily to these new capabilities but kept also adapting throughout the war.

Farragut accomplished feats of naval warfare on a scale and at a degree of difficulty never previously attempted.¹⁸ He, along with his fleet of 17 assorted steamships, including “screw sloops,” carrying 154 advanced guns, forced the surrender of the Confederacy's largest city and port, New Orleans. He did this by running a squadron past the forts downstream, moving this squadron up the river, and forcing the surrender of the city with the help of 100 of his marines. Farragut took advantage of the exceptional speed of steam propulsion, telling his subordinates, “I believe in celerity.”¹⁹ Upon taking New Orleans, Farragut was assigned to gain control of the southern Mississippi, with the goal of extending Anaconda. His planning and conduct of large-scale naval warfare on strategic waterways with exceptional speed and maneuverability were important contributions at the dawn of the revolution in naval affairs. Later, Farragut succeeded as

stunningly in bringing Mobile Bay under Union control, despite a formidable array of Confederate torpedoes (mines), which he is said to have loudly “damned” as he sped through them.

While Farragut was opening the southern Mississippi, Andrew Foote, commander of the Union's western gunboat flotilla, teamed with then-Brigadier General Grant to open Tennessee by river to Union control. Foote did this by devising and implementing, with Grant, a level of army-navy collaboration without precedent—a major contribution to the revolution in naval affairs and ultimately the principal American way of war. Grant himself described how Foote was in “perfect agreement” on how to take Fort Henry, on the Tennessee River, and nearby Fort Donelson, on the Cumberland.²⁰ Bombardment from Foote's fleet deserves primary credit for Fort Henry's capitulation—land forces arrived after the fort succumbed—and he played a supporting role in the subjugation of Fort Donelson 10 days later. With neither officer having authority over the other, Foote and Grant formed a partnership of trust, which has remained vital to jointness ever since.

The Navy Department's leading ordnance expert, Dahlgren, invented the eponymous gun, which excelled during the war. Though muzzle-loaded and smooth-bored, it had a bulbous breech that permitted immense explosive force and, thus, greater distance, accuracy, destructive force, and crew safety than heavy guns to that point. Promoted to rear admiral, Dahlgren was assigned to take or neutralize Charleston, cradle of the Civil War and protected by several forts that had been invincible to previous attempts. He sent monitors within 300 yards of Confederate batteries, while USS *New Ironsides*, a wooden-hulled ironclad with unmatched firepower, bombarded from off the coast. Two months of naval bombardment forced the abandonment of Charleston's forts, effectively ending the city's use by blockade-runners.²¹

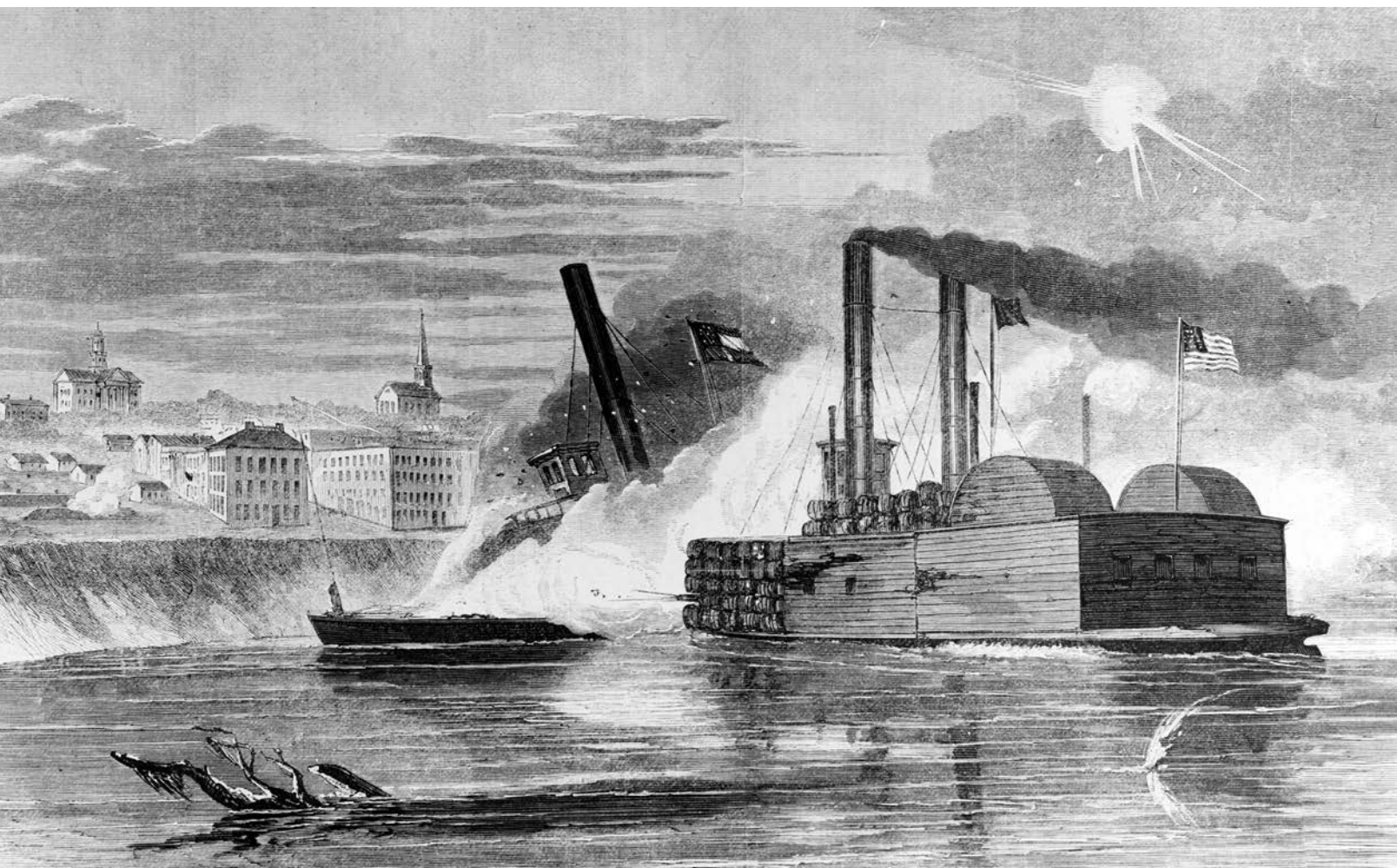
Welles was tapped to be secretary of the Navy because he supported Lincoln in the election of 1860. Assisted ably by Fox, Welles would forge the Union Navy into

a large, modern, and effective fighting force. It was the responsibility of Welles and Fox to create the capabilities, in quality and numbers, to carry out Anaconda, even as it became more challenging in the face of the South's response. USS *Monitor* was constructed at their direction, and the industrial mobilization they managed overpowered Confederate capabilities. Welles rewarded excellence and creativity in his officers, promoting Farragut, Dahlgren, Foote, and Du Pont to the new rank of rear admiral because of their success in leading change.

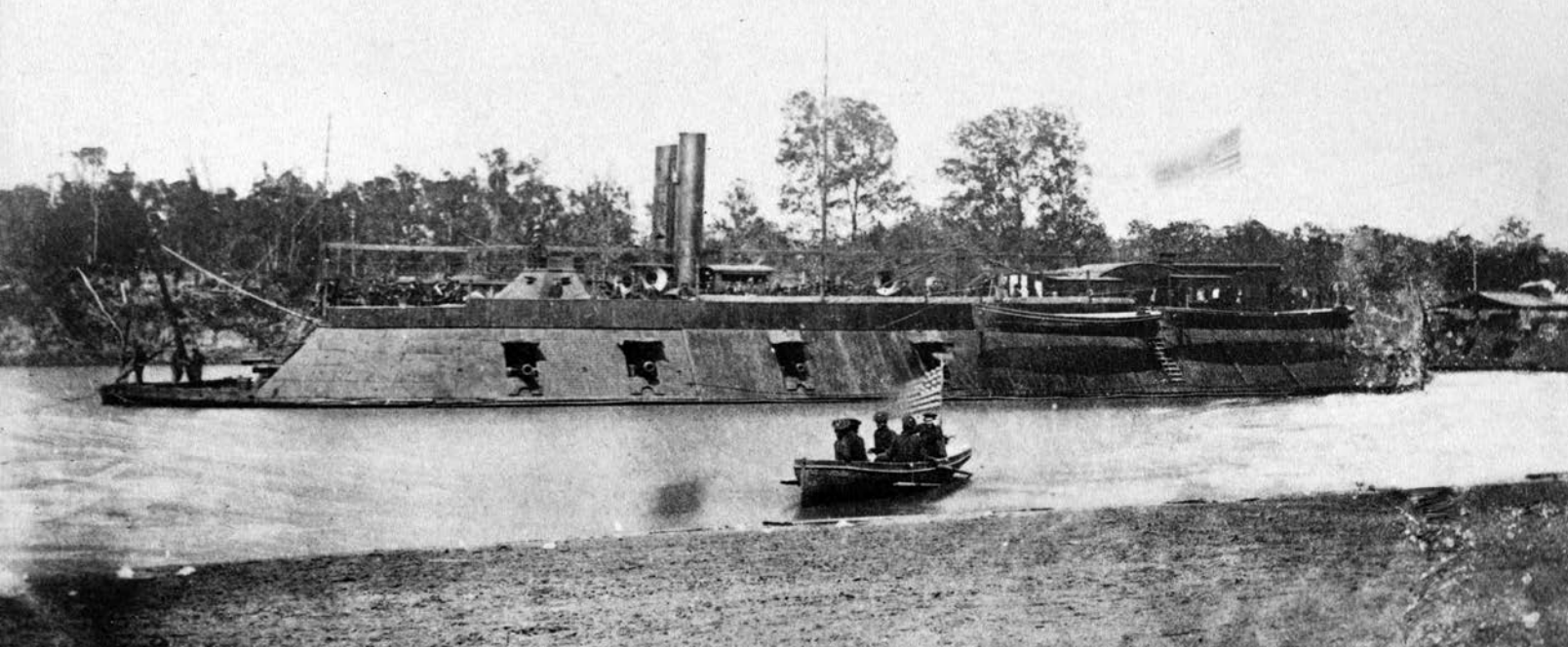
One of the key features of the Civil War's revolution in naval affairs was the feedback loop linking warfighters and those developing capabilities. To illustrate: in July 1864, Navy Secretary Welles sent a report titled *Armored Vessels* to Congress. Here are highlights:

- Rear Admiral Louis Goldsborough praised the rotating turret, recommended that all ironclads be armed with rifled Parrott guns and with rams, noted their vulnerability to plunging fire, and was skeptical about their invulnerability and seaworthiness.
- Rear Admiral John Dahlgren compared the virtues of the *Monitor* class to those of the *Ironsides* class, concluding that the classes had different attributes and were both needed. The monitors were more maneuverable in shallow waters and had better all-around protection, whereas the *Ironsides*-class warships could deliver more ordnance. He noted the beating that the monitors took during two months on station at Charleston and stressed the need for nearby repair facilities.
- Rear Admiral David Porter championed John Ericsson's monitor for its simplicity and effectiveness for both harbor protection and riverine duties. He was pleased that *Monitor*-class ships were being produced in Cincinnati for riverine use. He recommended modest improvements in armor but in general stressed their value as compared with that of the Pook gunboats at his disposal.
- Commodore John Rogers noted the *Ironsides* class's crew comforts and ability to move under sail if needed but stressed the *Monitor* class's thick iron for survivability and its heavy 15-inch guns for lethality.²²

The Union had an ample supply of naval officers. Some 400 graduates of the U.S. Naval Academy served in the



Engraving published in *Harper's Weekly* in 1863 depicting attack by Federal ram USS *Queen of the West* on Confederate steamer CSS *Vicksburg*, off Vicksburg, Mississippi, February 2, 1863 (Naval History and Heritage Command)



U.S. Navy City-class ironclad gunboat USS *Pittsburgh*, on western river, during Civil War (Library of Congress/Naval History and Heritage Command)

Union Navy, compared with 95 in the Confederate Navy. The Union Navy also had a cadre of experienced Sailors. While native-born Whites made up the majority, there were significant percentages of free (or freed) Blacks, plus Irish, British, and German immigrants. These crews were integrated, highly responsive to officers and petty officers, tough, and willing to take on new missions as strategy and leaders required.

Confederate Improvisation

The American naval strategist Alfred Thayer Mahan opined that the Confederacy was doomed for lack of a navy.²³ He theorized that any country with a long coastline and dependence on sea trade ought to have a capable navy, lest it fall victim to an opponent with one. He thought that the Union's Anaconda strategy would have failed had the Confederacy possessed a navy to defend its water frontiers. The South's long coastline and many harbors and inlets would have favored a stronger Confederate navy; given the South's relative weakness, it favored the Union Navy.

Why did the Confederacy not have, or try to build or buy, a navy commensurate with its size, ambition, and reliance on international commerce? As noted, the South, like the North, was unprepared for war on the heels of Lincoln's election. Yet the North proceeded with massive efforts to build a strong modern fleet. If the North's strategy was to flatline the

South's economy, why did the South not see the danger and act to prevent it?

There was a decidedly less robust seafaring culture and competency in the South than in the Northeast, which was steeped in maritime tradition and shipbuilding. The Confederacy lacked adequate shipbuilding capacity, and some of its yards were captured. It produced little iron and was unable to build steam engines. Most important, the Confederacy's highest priority by far was to field and sustain land forces. It spent just 10 percent of its wartime budget on naval capabilities, even as the lack of such capabilities was causing severe economic and strategic losses.

Though the Confederacy made do with minimal naval forces, it did have a resourceful naval leader in Secretary Stephen R. Mallory. As a former U.S. senator from Florida and chairman of the Naval Affairs Committee in the 1850s, he had championed U.S. efforts to convert sloops and frigates to steam warships. Because Mallory knew the South could never match the Union Navy, he championed improvisation.

The Confederates became skilled at laying mines to impede Union operations. These were very effective at slowing Grant's move toward Vicksburg. Mines in Charleston's harbor kept Du Pont from taking the city by sea. Defenders at Mobile Bay used mines to channel Farragut's fleet toward Fort Morgan's guns, though to no avail.

Despite metal-making and engineering shortages, the South did acquire some 20 ironclads to defend its ports and rivers. First was CSS *Manassas*, soon to be joined by others, including CSS *Louisiana*, *Mississippi*, *Atlanta*, and *Arkansas*. But it was the converted USS *Merrimack*, CSS *Virginia*, that made history by engaging in the war's first ironclad battle, with USS *Monitor*, in 1862. This fight was well heralded as a "giant step in the revolution in naval warfare."²⁴ However, as noted, most Confederate ironclads were eventually sunk, captured, or scuttled to avoid seizure. The South's capacity for industrial mobilization was negligible—cotton was king.

On the Mississippi, the Confederacy converted commercial steamboats into rams. Protected by thin armor and cotton bales, each such vessel had only one gun—a ram reinforced with iron—as its main weapon. Rams had existed for millennia, but with steam power, their superior speed made them deadlier. Some Union officers acquired what they called "ram fever," a fear of what the rams could do to gunboats.

The height of Confederate ingenuity was a privately built submarine, CSS *H.L. Hunley*, which was the first submarine ever to sink an enemy ship when it sank USS *Housatonic* in Charleston's outer harbor. The sleek 40-foot vessel, made of iron, had a crew of eight, a hand-crank propeller, ballast tanks, hand pumps, and a torpedo at the end of a 22-foot

spar triggered to detonate at contact. Early efforts to experiment with electric and steam-powered submarines were abandoned. *H.L. Hunley*'s top speed was only 4 knots. In its successful attack on *Housatonic*, its own crew was killed, probably from the concussion of the explosion.

Southern improvisation alone, however, does not qualify as a revolution in naval affairs. Confederate leaders were prepared to experiment because they had little choice. The Confederacy was the first to deploy an ironclad, a submarine, and mines. After the Civil War, many of the innovations made by Mallory and his colleagues would be adopted by the U.S. Navy, thus contributing to the naval revolution that would make the United States the sort of sea power advocated by Mahan.

Subsequent Revolutions in Naval Affairs

The U.S. Navy was the world's largest in 1865, but it was largely moth-balled after the Civil War, for lack of an enemy. Yet study of its revolution spread. Foreign powers—Great Britain, France, Russia, Japan, and newly formed Germany and Italy—hurtled into competition for colonies. Strong battle fleets were their main capabilities for both colonizing and competing.²⁵ These nations began to build large, turreted, oceangoing ironclads. Soon, Great Britain was constructing very large armored warships.²⁶ British and German battleships, battle cruisers, and destroyers built and sent into World War I were direct descendants of the ships commissioned by the Union for the Civil War. Even the British and German dreadnoughts, improved with steam turbines, onboard electricity, radio communications, and reinforced cladding, were grandchildren to the warships built for the American Civil War some 50 years earlier.

The submarine underwent a less linear development between the Civil War and World War I, from the small, hand-cranked, spar-mine-armed CSS *H.L. Hunley* to the German U-boat of 1914–1918, which was steam-propelled, larger, much faster, and much more dangerous for its adversary with its

self-propelled torpedoes. At the same time, amphibious warfare, which figured prominently in the Civil War, was a colossal failure in World War I, when an ill-advised Winston Churchill-inspired British-led attempt to take the Gallipoli Peninsula and gain control of the Turkish Straits ended in an Ottoman victory and a combined loss of half a million lives. Overall, World War I did not bring about a revolution in naval affairs.

Although there have been numerous important naval innovations since the American Civil War, only three genuine naval revolutions conform to the Civil War paradigm of strategy and technology parenting new capabilities, which were then multiplied by industrial mobilization and used effectively by visionary leaders.

The advent of fixed-wing airplanes led to a such revolution starting in the 1920s, which promised greatly increased lethality at far distance. With Europe temporarily at peace, U.S. geostrategic attention shifted to the Pacific, where the rise of Japanese militarism and appetite for East Asian resources spelled danger to U.S. interests. At that time, Army General Billy Mitchell, a proponent of bombing, argued and demonstrated that surface ships, even battleships, could be quickly sunk by air attack.²⁷ He was court-martialed in 1925 for calling Army and Navy leaders “almost treasonable” for investing in battleships instead of aircraft carriers. Revolutionary leadership often requires courage along with vision.

Despite the merciless reaction to Mitchell's impertinence, the case for carriers prevailed, partly because Japan was showing strong interest in them. Just as the United States commissioned its first carrier, in 1922, so did Japan. At first, the carrier was regarded by U.S. admirals as helpful to extending surveillance hundreds of miles so that battleships could close in for the kill. But then, steam-powered catapults and arresting gear were developed to help heavily armed planes take off, deliver substantial ordnance, return, and land, making the carrier the principal instrument of long-range attack. Despite persistent opposition from the battleship lobby, aircraft carriers would largely decide World War II in the Pacific.

Wartime industrial mobilization was breathtaking: the United States built 105 carriers, 40 of them large-deck ones.

In contrast to dreadnought warfare, carrier warfare was “offense-dominant.” In the biggest naval engagement of World War I, the Battle of Jutland (1916), neither Great Britain nor Germany lost *any* of the total of 44 dreadnoughts in the fight; essentially, their gunnery was no match for their armor. At the Battle of Midway (1942), of the seven carriers employed by Japan and the United States, five—four Japanese and one American—were sunk, due mainly to air attack. The revolution brought about by naval aviation shifted the advantage at sea from defense to offense—which is just what the United States needed to recover control of the Pacific and take the war to Japan.

After winning World War II, the United States found itself with global responsibilities and threats that demanded sustained presence and patrolling by submarines as well as carriers in distant regions. Nuclear-fission technology offered the answer. Led by Admiral-to-be Hyman Rickover, the United States developed and equipped all of its submarines and some of its carriers with nuclear propulsion. Reactor refueling was needed every decade or so, compared with every month or so for fossil-fueled ships.²⁸ Superiority in nuclear-powered attack and strategic-missile submarines would make the United States the leading global sea power and give its strategic triad an invulnerable leg.²⁹ Outfitting the submarine fleet with reactors required mobilization of a specialized new industry. As for Rickover, admirers on Capitol Hill had to keep the Navy from cashiering him for insufficient collegiality.³⁰

By the end of the bipolar world, with the Soviet Union's days numbered, the United States found it necessary to project military power to regional contingencies, notably in the Persian Gulf and the Balkans. To gain access for fast intervention with low casualties, the Navy and its sister Services responded by deploying dispersed forces and precision-guided munitions during the 1990s. This required what in Pentagon-speak is considered networked “command, control,



Members of USS *Miami* crew on forecastle, ca. 1864–1865; Frank W. Hackett, former officer of the ship, wrote in 1910: “The officer standing in the background, at the extreme prow of the ship, is W.N. Wells, Executive Officer. The man in the foreground with his arm on the nine-inch gun is White, the gunner. Sergeant of Marines, Stanley, is sitting in the foreground, near the capstan” (Naval History and Heritage Command)

communications, computers, intelligence, surveillance, and reconnaissance.” Preceding this development, and mainly outside the government, the skyrocketing commercial demand for distributed processing gave rise to data networking—just what integrated, joint, power-projection operations needed. It took the decade of the 1980s for the digital revolution to transform the military. A dazzling U.S. victory in the Gulf War revealed a new capability: information.

While the leaders of data networking were chiefs of the commercial computer and telecommunications industry, several senior naval officers had the imagination and nerve to promote the idea of networked forces. One was Vice Admiral Arthur K. Cebrowski, an intellectual who ran the Pentagon’s Office of Force Transformation in the early 2000s. Another was Vice Admiral Jerry O. Tuttle, who had the more hands-on job of creating a joint network-based operational

command and control system. A third was Admiral Bill Owens, an influential Vice Chairman of the Joint Chiefs of Staff, who wrote an important article in *Foreign Affairs*³¹ and was a prime mover of the Pentagon’s seminal *Joint Vision 2010*. There was also Rear Admiral Wayne E. Meyer, who adopted networking to integrate shipboard missile defense. These officers and their acolytes guided the U.S. Navy to overcome its long-held belief in unit autonomy. Of the many lessons of the digital naval revolution, among the most important is that the U.S. military needs technology designed for civilian use—for example, the Internet.

The Case for Another Revolution

With information technology vital, ubiquitous, and in constant flux, the United States must be poised for a new naval revolution, as part of what is known as joint, all-domain warfare.³² The U.S.

military’s highest development priority today is to integrate forces with shared and timely information. Like other revolutions, this one starts with strategy: thwarting China’s growing challenge to American power in the Pacific. The magnitude of this challenge dictates learning from prior revolutions—yes, all the way back to the Civil War.

Parallels between then and now are striking. The Union adopted a strategy to strangle the Confederacy, only to discover that its capabilities were inadequate to execute it. Today, U.S. strategy calls for maintaining a superior military presence in the Western Pacific, while new Chinese capabilities are making such a presence untenable. With current U.S. strategy and capabilities, the trend is unfavorable. Unless it is prepared to abandon its influence, alliances, and warfighting edge in that vital region, the United States must embark on a new strategy enabled by new technology.



The Monitor and Merrimac: The First Fight Between Ironclads, chromolithograph of Battle of Hampton Roads, Louis Prang & Company, 1886 (Library of Congress)

Beijing seems determined to retake what it considers historically sovereign territory and seas, stripped from China by imperial powers when it was weak. Doing so would restore Chinese supremacy in East Asia. Perceiving, with good reason, that U.S. military power in the Western Pacific is its principal obstacle, China has developed and deployed quiet attack submarines and maneuverable anti-ship missiles, which would make the Western Pacific a keep-out zone for U.S. forces. Now, as China's race with the United States in advanced information technology heats up, it is putting in place extended-range sensing systems to locate, track, and target U.S. forces at increasing distance from China. Just as the aircraft carrier was crucial in a prior naval revolution—to counter Japan and to project U.S. power—another revolutionary approach is now crucial to dealing with this new challenge.

The concept now coursing through Pentagon corridors is to deploy a joint force that is more dispersed, diverse,

elusive, and unmanned than today's, thus confronting China with a very different and harder targeting challenge. The central nervous system of this emerging U.S. force is to be a network to guide and integrate operations across all military Services in all realms: land, water, air, space, and cyberspace.³³ This network will rely mainly on constellations of satellites and surveillance drones. The system's essential capability is information gathered, processed, and distributed seamlessly and fast.

As this strategy forms, the Navy will have a huge role, though it must transition toward smaller and more numerous surface vessels, some of them unmanned, with long-range strike weapons—ballistic, cruise, hypersonic—as well as submarines outfitted with such missiles. While aircraft carriers will remain vital in other regions of U.S. interest, they will become Pacific launch platforms for drones and aircraft with long-range weapons so that they need not steam close to China. The Navy will also need to keep up with constantly improving

network software, hardware, and bandwidth that will unify all U.S. forces.

The U.S. strategy demands no less than another revolution in naval affairs, just as other of the Nation's military Services are entering parallel transitions. The requisite technologies are being developed mainly by non-defense innovators, from very large to very small: artificial intelligence (AI), complex autonomous systems, and quantum computing and communications, to name three.

Before assuming that the U.S. Navy and other Services can carry out a revolution to counter China based on civilian technology, certain issues need attention. First, the prospect of unmanned warships run by AI raises concerns about who, or what, controls the use of force. Second, deemphasizing large-deck aircraft carriers in a vital area runs counter to naval, and national, instincts. Third, disincentives for innovative civilian firms to do business with the Pentagon must be demolished, despite political and bureaucratic resistance. Meeting

these challenges will require officers of uncommon ability, willing to joust with forces of tradition and to take risks, including to their own careers.

It is unclear whether the Navy is flexible and imaginative enough to embed its fleet within an integrated all-domain force, where its ships are nonautonomous nodes on a joint network. Recall the Navy's attachment to battleships in the run-up to World War II. Recall the court-martial of Mitchell and ostracism of Rickover for heresy. Recall how Farragut, Dahlgren, Porter, and Welles led the Civil War naval revolution.

The matter of leadership today is complicated by the preeminence of jointness in combat, command and control, force planning, and even technology development. Senior Navy officers, like those of other Services, are increasingly expected to serve in joint assignments. Conversely, leaders of joint organizations from other Services may have as much influence on naval roles and requirements as Navy officers. The notion of a revolution in naval affairs is nowadays hard to disentangle from that of a larger revolution in military affairs. The next Farragut could be in the Army.

One senses that the Chinese threat is motivating senior officers of all Services to exhibit the creativity and verve to guide a new, information-based joint revolution spanning all domains. Less clear is whether they have adequate political top cover from a U.S. Government preoccupied with such other pressing matters as a pandemic, climate change, education, voting rights, and immigration.

Conclusions

The Civil War was the fulcrum of American history: It caused untold violence, destroyed the South's horrific culture and economy of slavery, and gave freedom followed by citizenship to 4 million Americans. It also restored the Union states, which would go on to build unmatched industrial might. Likewise, the Civil War was pivotal in naval history, replacing wind-propelled wooden ships with steam-propelled ironclads. Eventually, the U.S. Navy became an instrument of American power across the globe.

This national and naval narrative began when the Union's Anaconda Plan to cripple the South proved unachievable until old ships, obsolete doctrines, and uninspired officers were replaced. By war's end, mobilized Northern shipyards were rapidly launching ironclads with steam power and accurate guns.

From the top down, Union officers and crews escaped the gravity of tradition. Then and since then, the constant of naval and other military revolutions is the creativity and impatience of leaders. Across several naval revolutions, individuals such as Farragut, Mitchell, Rickover, and Owens brought change by exploiting technology, as Americans are wont to do. Revolutionary champions who emerge today will deserve a place in this pantheon. It behooves today's leaders to study how their forebears did what they did. **JFQ**

Notes

¹ In December 1860, the U.S. Navy had just 7 screw frigates and 10 first-class steam sloops, plus 18 second- and third-class steamers. None were ironclads. See *Register of the Commissioned and Warrant Officers of the Navy of the United States, Including Officers of the Marine Corps, and Others, for the Year 1861* (Washington, DC: Department of the Navy, 1861).

² For details on Civil War naval developments, see James M. McPherson, *War on the Waters: The Union and Confederate Navies, 1861–1865* (Chapel Hill: University of North Carolina Press, 2012); and Kevin Dougherty, *Strangling the Confederacy: Coastal Operations in the American Civil War* (Philadelphia: Casemate, 2009).

³ See Robert McNamara, "Overview of the Anaconda Plan of 1861," *ThoughtCo*, March 7, 2021, <http://thoughtco.com/anaconda-plan-definition-1773298>; Gary Gallagher, "The Anaconda Plan of the American Civil War," transcript, from the lecture series "American Civil War," *Wondrium Daily*, April 25, 2020, <https://www.wondriumdaily.com/the-anaconda-plan-of-the-american-civil-war/>; and Ken Stover, "Anaconda Plan," Civil War Academy, <https://civilwaracademy.com/anaconda-plan>.

⁴ McPherson, *War on the Waters*, 32.

⁵ Dougherty, *Strangling the Confederacy*, 61–67.

⁶ See Dougherty for a detailed history of joint Union Army-Navy operations.

⁷ McPherson, *War on the Waters*, 219.

⁸ *Ibid.*, 52–53.

⁹ "U.S. Patent Activity: Calendar Years

1790 to the Present," U.S. Patent and Trademark Office, 2023, https://www.uspto.gov/web/offices/ac/ido/oeip/taf/h_counts.htm.

¹⁰ The turbine was not used in steam-propulsion plants until 1894.

¹¹ E.B. Potter and Chester Nimitz, eds., *Sea Power: A Naval History* (New York: Prentice-Hall, 1960), 265.

¹² Dougherty, in *Strangling the Confederacy*, thoroughly examines joint Army-Navy operations in the Civil War.

¹³ McPherson, *War on the Waters*, 169.

¹⁴ *Ibid.*, 176.

¹⁵ Williamson Murray and Wayne Wei-siang Hsieh, *A Savage War: A Military History of the Civil War* (Princeton: Princeton University Press, 2016).

¹⁶ Benjamin T. Arrington, "Industry and Economy During the Civil War," National Park Service, <https://www.nps.gov/articles/industry-and-economy-during-the-civil-war.htm>.

¹⁷ McPherson, *War on the Waters*, 224.

¹⁸ *Ibid.*

¹⁹ *Ibid.*, 60.

²⁰ Ulysses S. Grant, *Personal Memoirs of U.S. Grant* (Cambridge: Belknap Press, 2017), 147.

²¹ McPherson, *War on the Waters*, 176.

²² From the library of James Townsend, *Report of the Secretary of the Navy in Relation to Armored Vessels* (Washington, DC: Government Printing Office, 1864), 571–594.

²³ Alfred Thayer Mahan, *The Influence of Sea Power Upon History 1660–1793* (Boston: Little, Brown and Co., 1890), 43–44. Mahan also opined that never had sea power played a more decisive role than in the "conflict which determined the course of world history."

²⁴ McPherson, *War on the Waters*, 104.

²⁵ For a cogent explanation of European naval strategies and competition in the run-up to World War I, see Clark G. Reynolds, *Navies in History* (Annapolis, MD: Naval Institute Press, 1998).

²⁶ Potter and Nimitz, *Sea Power*, 368.

²⁷ Mitchell persuaded the Navy to let aircraft bomb an ex-German dreadnought after World War I. It promptly sank.

²⁸ Reactor cores can last as long as 30 years, but standard practice is to replace them more frequently.

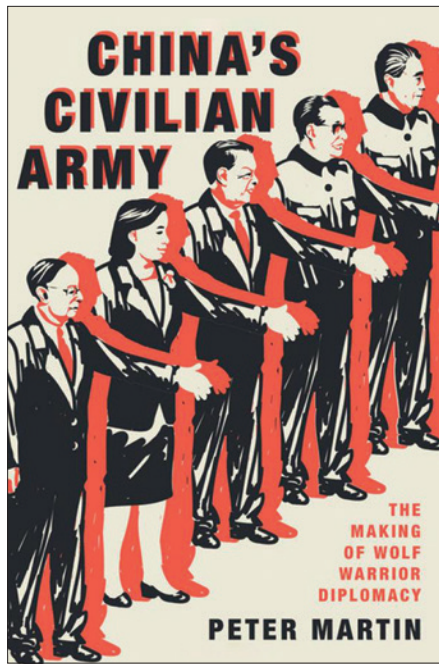
²⁹ Intercontinental ballistic missiles and strategic bombers also played a role.

³⁰ Theodore Rockwell, *The Rickover Effect: How One Man Made a Difference* (Annapolis, MD: Naval Institute Press, 1992).

³¹ Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs*, March/April 1996.

³² "All-domain" refers to land, sea, air, cyber, and space.

³³ This network is called Joint All-Domain Command and Control.



China's Civilian Army: The Making of Wolf Warrior Diplomacy

By Peter Martin

Oxford University Press, 2021

298 pp. \$27.95

ISBN: 9780197513705

Reviewed by Ian Forsyth

George Schultz, the U.S. Secretary of State from 1982 to 1989, equated diplomacy to gardening: long-term cultivation and maintenance of a healthy relationship that slowly but reliably bears fruit. Peter Martin's *China's Civilian Army: The Making of Wolf Warrior Diplomacy* depicts a Chinese diplomatic corps that has intermittently subscribed to this philosophy. This clear and engaging book is an enlightening blend of domestic People's Republic of China (PRC) politics, foreign policy practice, and diplomatic history with a fair amount of Zhou Enlai biography thrown in. Zhou was China's first foreign minister (FM) from its founding in 1949 to when he stepped down as FM in 1958.

Martin is a political reporter for Bloomberg News and spent several years as a correspondent in the PRC as well

as having studied at Peking University. *China's Civilian Army* devotes roughly half of its pages to the origin of the PRC diplomatic corps and Zhou. It tracks the evolution of its diplomats, who were disciplined, committed Communists, modeled in structure and spirit on the People's Liberation Army, hence the book title. They approached diplomatic assignments, conferences, and even basic meetings with little to no appropriate social science training or much host-country knowledge. Instead, they possessed a single-mindedness borne out of national insecurity and a lack of trust for one another in the field that was often self-defeating. The book also highlights the role of (often tumultuous) domestic Chinese politics, which could be crippling to its diplomatic efforts. It concludes in the 21st century, where undeniable Chinese growth and power, with approval from Xi Jinping, spawned a generation of PRC diplomats who are combative, caustic, and sometimes petty (the exact opposite of Secretary Schultz's prescription). This aggression was nicknamed "wolf warrior diplomacy" (战狼外交) after a series of recent popular Chinese war movies.

Martin draws on the memoirs of over 100 retired American and Chinese diplomats, State Department and CIA archives, as well as his own career as a China correspondent for Bloomberg to tell this story. His research captures the nexus of political science, international relations, as well as history and biography, so it could claim residency in any of these disciplines.

Although *China's Civilian Army* starts off as history with some biography, it evolves into a study of what drove and incentivized China's diplomatic interactions. While the argument is not explicit, Martin presents a dynamic in which first and foremost China's diplomats are concerned with adhering to priorities of Chinese high politics. Through the PRC's first 20-odd years, these diplomats were more information officers than anything else. They declared China's official line in single direction "dialogues" with their hosts. While all diplomats are beholden to their countries' politics to varying degrees, Martin depicts a

community where political loyalty to Beijing and recitation of Beijing's truths were supremely valued. This made Chinese diplomacy exceedingly challenging during the Great Leap Forward and Cultural Revolution. Along those lines, Martin reveals that despite how influential or charismatic certain FMs might be (for instance, Zhou, Qian Qichen), it is the Party chairman who sets the tone, particularly if that chairman is especially paranoid (Mao Zedong, Xi). Martin also observes that the bulk of the wolf warrior vitriol has been directed at middle powers such as Australia and Sweden.

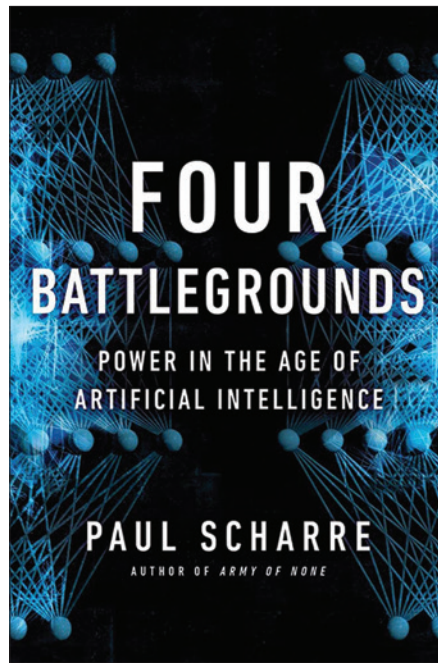
Another argument Martin implicitly advances is that the current wolf warrior diplomacy is not unprecedented; it has ebbed and flowed over the decades but never completely disappeared. Contemporary wolf warriors such as former FM spokesperson Zhao Lijian and former ambassador to Sweden Gui Congyou shock audiences with their barbed statements, but they are not the first of their kind. The difference between modern and prior wolf warriors is that the original warriors' combativeness was borne out of insecurity and the need to carve a niche for a newly created country. In contrast, contemporary warriors are brimming with the confidence of a country whose rise has been remarkable, whose power is undeniable, and whose respect has heretofore been unfairly denied. Martin describes how certain PRC elites are uncomfortable with this chest-thumping, but it still plays well with the PRC online populace, so such bravado is rewarded on a certain level.

While Martin does not make predictions or assert conclusions, the logical inference he draws is that because China is a major power, these diplomats will be ever-present though maybe not ubiquitous. Martin is professional enough not to wear his heart on his sleeve, but he clearly sees these diplomats as obnoxious and even dangerous at times. He highlights their impressive language skills and prestigious formal education but makes clear that such expertise and professionalism is often discarded if not outright rejected by their FM superiors for the sake of political expediency.

China's Civilian Army is valuable because it could assist the joint force in its efforts to understand China's foreign policy and the role of domestic politics in its foreign policy behavior by highlighting the trends and dynamics of China's diplomats. It is effective at illuminating the connection between Chinese senior leadership, China's global position in terms of power, and how these drivers impact Chinese formal and informal diplomacy. It is also accessible for non-Sinologists and does not require a strong China background to understand it, though a China background does help. It is also very well written with clear, informative prose.

Recent headlines seemingly point to an ebb in wolf warrior diplomacy. Notorious wolf warrior Zhao Lijian has been shifted from Foreign Policy Spokesperson to the Deputy Director for Boundary Affairs; he may or may not be demoted but he certainly is muzzled. Xi and President Joe Biden had a seemingly positive summit in Bali last November at the G-20. New FM/outgoing ambassador to the United States Qin Gang departed with warm statements for his hosts. Is this a tactical retreat by China's civilian army, or is it a broader philosophical change? It is more likely that China's domestic pressures, such as containing COVID-19 and reigniting its economy, compel Xi to prioritize stability and not unnecessarily alienate other powers, particularly the United States. Research by Dan Mattingly and James Sundquist of Yale shows how unhelpful China's wolf warrior tactics are. It is advantageous for China to attend to its diplomatic garden after years of neglect. Yet based on Martin's research, China's wolf warriors will inevitably return in one form or another, particularly given China's size, stature, and power. **JFQ**

Ian Forsyth is an Assistant Professor of National Security Studies in the Dwight D. Eisenhower School for National Security and Resource Strategy at the National Defense University.



**Four Battlegrounds:
Power in the Age of
Artificial Intelligence**

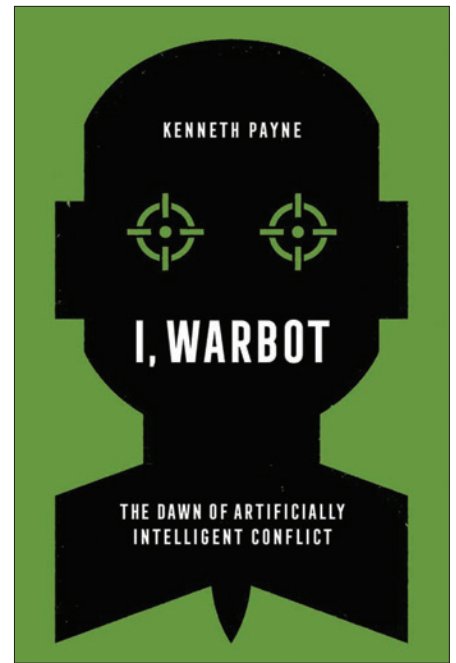
By Paul Scharre
W.W. Norton & Company, 2023
496 pp. \$32.50
ISBN: 9780393866865

**I, Warbot: The
Dawn of Artificially
Intelligent Conflict**

By Kenneth Payne
Oxford University Press, 2021
280 pp. \$29.95
ISBN: 9780197611692

Reviewed by Frank G. Hoffman

The rollout of Chat GPT-3 by OpenAI in late 2022 caused a storm of controversy. The new software created seemingly authentic and detailed answers to queries, generated passable drafts of student essays, and even managed to pass a college exam at the Wharton Business School. But some of the chatbot's responses were also inaccurate, inappropriate, and deeply flawed. The updated version GPT-4, released in March 2023, did little to alleviate concerns about how far and how fast this technology could take us.



Here again the rapidly developing field of artificial intelligence (AI) brought out a spate of spurious claims and serious concerns. Given the purported progress being made in computational intelligence, it is imperative that the Armed Forces be attentive to understanding what AI can and cannot do within our professional sphere. There is little doubt that AI will bring about profound changes in the conduct of warfare, and equally little agreement on just what those changes will be.

Two recent books, *Four Battlegrounds* and *I, Warbot*, will help readers sort out the hype from the hysteria. Both address the state of the art of today's AI and machine-learning technology with interesting anecdotes and insights drawn from intensive interaction with leading laboratories, critics, and scientists around the globe. Most importantly, they underscore what we should be wary of when incorporating AI into military institutions and operational practice.

Four Battlegrounds, penned by Paul Scharre from the Center for a New American Security, blends a pragmatic approach borne from his days as an Army infantryman with the perspective of a veteran Pentagon policy wonk. This is Scharre's second major work on the topic. His initial book *Army of None*:

Autonomous Weapons and the Future of War (W.W. Norton, 2018) was widely acclaimed. That volume zeroed in on the ethical implications of autonomous weapons. His grasp of the implications was not only sobering but also overly hopeful about international norms and arms control. It was an impressive effort that this reviewer did not think would be soon surpassed.

Four Battlegrounds proved that wrong in short order. Scharre covers the exciting advances of the last 5 years in an accessible style. He has produced a well-balanced and detailed assessment of the state of the art and a useful critique of just how fast and far the Pentagon is moving. Overall, the author takes a prudent approach when it comes to AI's dramatic potential.

His title is drawn from four key considerations that will determine the pace and scale of our ability to leverage AI productively. Success will require progress in each of the four "battlegrounds":

data, computing power, human talent, and institutions. Large-scale models are now fueled by massive amounts of data, hoovered up and stored for training algorithms. Data is the fuel for the AI revolution. Powerful computers with ever more sophisticated chips are coming online, but the fabrication of these slivers of silicon depends on a fragile production chain. While silicon wafers constitute a critical element of the cyber ecosystem, the most precious asset is human talent. Scharre argues that developing human capital should be a higher priority for U.S. strategy, reinforcing a point made by the National Security Commission on Artificial Intelligence.

The final battlefield is also an area ripe for reform. Ultimately, it is not the technology itself that will determine success; it depends on institutions that adapt their processes, metrics, and structures to best apply AI and machine learning. The author suggests we have a way to go if we want to move past hardware and platforms and accept data and algorithms as units of combat power. More critically, he excoriates the bureaucratic processes that retard agile development of AI capabilities. The greatest barrier to adoption

is not computing power or creative new algorithms. The most significant hurdle is the government's own acquisition bureaucracy and red tape. An encrusted system designed to eradicate risk and curtail budgetary fraud extends the proverbial "valley of death" for startup companies and strangles them in the cradle as they try to scale up. To Scharre, the government's own system is more lethal to our success at innovation than any "pacing threat."

Scharre warns that "If the United States moves too slowly it could cede military dominance in a critical new technology to a rising and revisionist China" (6). At the same time, the clearest message in *Four Battlegrounds* is a warning: We should not let the fear of falling behind leading countries alter our risk tolerance about "the appropriate balance between fielding new AI systems and ensuring that these systems are robust and reliable" (257).

I, Warbot is more philosophical but no less insightful. The author, Kenneth Payne, works for the United Kingdom defense establishment and previously penned an intriguing book on AI's impact on strategy titled *Strategy, Evolution, and War: From Apes to Artificial Intelligence* (Georgetown University Press, 2018). He brings a unique perspective on the nexus of psychology and strategy, which is a valuable lens for seeing the benefits and barriers of employing AI and machine learning in the military.

Payne explores the creative capacity of AI programs with a typology of three different kinds of creativity. He finds that AI supports only the first two types: exploratory and combinatorial. In these two forms, algorithms examine patterns and assess probabilities from existing data. This is the kind of creativity exhibited by the winning poker-playing computer program Libratus or the earlier AlphaGo program that beat a world champion Go player convincingly. Where computers and AI systems fall short is in the third category—transformative creativity. This is the kind of intelligence needed when facing a novel problem or when an old problem requires solutions that have not yet been conceived. These situations

require more than predictive computation and more imagination. As Payne stresses, AI programs may be tactically brilliant in the narrow task each is designed for, but they cannot connect dots or "understand" a novel situation that they have not been programmed for or provided a data set to learn from.

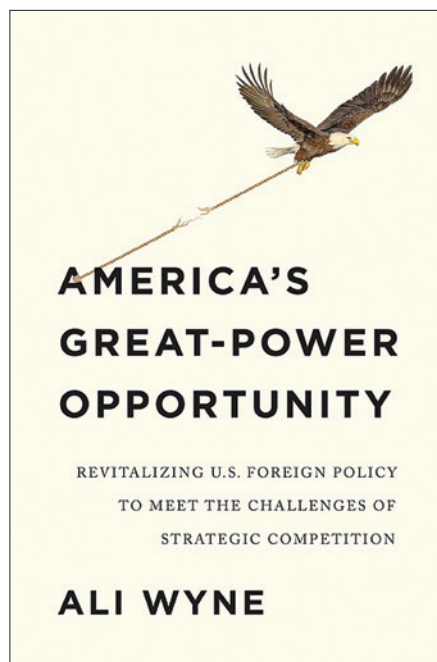
Both authors promote human-machine teaming instead of the overdramatized fascination with autonomous systems. "The most effective military systems," Scharre concludes, "will be those that successfully combine human and machine decisionmaking and the most effective militaries will be those that find ways to optimally employ human-machine teaming" (264). Payne readily agrees at the tactical level but argues they will be strategically naïve due to their lack of empathy and transformational imagination.

The best and most challenging chapter in *I, Warbot* deals with human-machine teaming. Payne goes deep into the potential of centaur teams, which combine human decisionmakers and AI support systems, initially advanced by Gary Kasparov (the Russian chess master who famously lost a match to IBM's Deep Blue a quarter-century ago). Payne recounts several experiments and government wargames where such centaur teams engaged in strategic interactions. Payne's speculations are not conclusive, but he suggests that a pairing of a human and AI systems may produce synergistic advantages along with some detracting interactions. He aptly perceives the dramatic acceleration of tactical activity in war that can be matched only by machine speeds, but he is also hopeful that AI can aid strategy formulation since it offers more time for collaborative and creative deliberation between senior leaders and augmenting support systems. But the interaction between human commanders (the source of curiosity, intuition, and transformational creativity) may be inhibited by decision support systems that might be reluctant to accept or interact productively with an AI system. This, he argues, warrants far more study. For now, and in the immediate future, "Warbots will make incredible combatants, but limited strategists" (181).

There are common conclusions between this engaging pair of authors. Both suggest that the introduction of autonomous systems is unlikely to change the nature of war. It is axiomatic to the U.S. military that war's essential nature is immutable, while the character of warfare (how war is conducted) is always changing. Scharre notes that the increased reliance on drones, uncrewed systems, and swarms reduces the role of humans at some levels of war. Yet humans will still initiate war, set out the policy aims, develop strategies, employ machines, make decisions, and even fight. Not surprisingly, Payne agrees. He does not envision the human element of war disappearing any time soon. "Even if machines make more decisions at the tactical level," Payne concludes, "war will remain something that is done by and to humans" (84).

Four Battlegrounds and *I, Warbot* are each outstanding, but together they offer complementary insights. Both authors raise the kind of hard questions and uncomfortable issues that we must face as this technology evolves. Both books will improve readers' AI literacy and deepen their critical thinking about how we approach AI in our respective domains. Accordingly, both books are highly recommended to the joint community and the larger strategic studies field on both sides of the Atlantic. The introduction of AI-enabled support has huge potential benefits to training for war; in the conduct of warfighting; and many support functions including intelligence, logistics, and cyber security. But real progress will be made only by seeking to employ AI responsibly, with rigorous attention to validation, and a healthy appreciation for how brittle the technology is today. This pair of books offers a valuable guide to the revolution that will increasingly define our economies and security in the coming years. JFQ

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



America's Great-Power Opportunity: Revitalizing U.S. Foreign Policy to Meet the Challenges of Strategic Competition

By Ali Wyne
Polity Press, 2022
234 pp. \$25.00
ISBN: 9781509545544

Reviewed by Thomas F. Lynch III

America's *Great-Power Opportunity* is a lucid, thoughtful assessment of the problems and the possibilities with the geostrategic formulation of Great Power competition (GPC). Ali Wyne frames a narrative that captures well the major debates from 2017 through 2022 surrounding whether GPC is a proper framework for understanding America's evolving geostrategic posture and how Washington's global strategy should respond. Wyne adds value to the prolific number of publications on GPC during 2021 and 2022 by recommending that Washington accept the new norm of competitive geopolitics with a positivist rather than a reactive strategic agenda. For Wyne, *America's Great-Power Opportunity* is to move beyond strategic reflexiveness

toward its two Great Power rivals while reaffirming America's global democratic example and evolving the present global order with greater ownership and participation from allies and partners.

Wyne's thrust in *America's Great-Power Opportunity* differentiates between GPC as a description of geostrategic reality and as a policy prescription for American strategy to prevail in such a reality. He comes down generally in favor of the former but deeply worried about the latter.

Although unduly tepid in his determination, Wyne correctly tells us that GPC is an apt descriptor for contemporary global politics, getting much right about today's world order, one that starkly changed over a decade from about 2008 to 2017. Strategic competition between rivalrous powerful states is a norm of human history. The period from 1992 to 2008 was a historic anomaly where preeminent American power dominated state-to-state relations and allowed Washington to alternatively woo or coerce mainly collaborative interstate dynamics. Over time, American power has relatively declined, and rivals Russia and China have grown in stature and assertiveness.

Moscow and Beijing now seek to translate Great Power capabilities in the pursuit of self-interested rules, norms, and procedures that do not align with those established and adhered to by Washington and its partners since World War II. Wyne tells us that this return to a new geopolitical normal is properly captured in the descriptive framework of GPC. Even though he occasionally slips when writing that America remains the lone world superpower, Wyne mostly accepts that the December 2017 National Security Strategy of the United States of America got it right when it advanced GPC as the new geostrategic reality, supplanting over three decades of American strategic focus on engaging the world for the purpose of enlarging the zone of liberal democratic states.

At the same time, Wyne worries that the GPC framework may be a setup for bad American strategy. He states that too many Americans focus on the word *competition* leading to a pair of dangerous

strategic premises: excessive external focus and hyper-reactivity to Great Power rival initiatives and provocation. Indeed, some proponents of GPC have written that proper American strategy must be focused intensely on and react to the moves by China and Russia as though parry-and-thrust competition is an imperative in and of itself. Wyne properly cautions that a more judicious balance for American strategy is necessary:

While Washington will increasingly have to contend with and manage the challenges posed by a resurgent Beijing and a revanchist Moscow, it should not pursue a foreign policy that is driven by or beholden to their actions. It should instead articulate a forward-looking conception of its role in the world, identifying cases where circumscribed competition with China and Russia might further that vision (19).

Wyne also contends appropriately that Cold War analogies for future competitive American geostrategy and foreign policy are misleading. He offers nine critical factors that make them wrong. Among the nine is the fact that the economies of the Cold War superpowers were barely interactive, while the American and Chinese economies are today intertwined to a degree unrivaled in recent human history. So too is Wyne's observation that the Cold War featured binary policy calculation—"I win, you lose"—while today's GPC is multipolar and the power losses by one are not automatic gains for the others. Modern Great Power rivalry is a far more complex and nuanced strategic challenge.

A worthy American competitive strategic framework, Wyne writes, requires a renewal within America paired with humble but persistent leadership of a broad array of like-minded states, capable of resisting Russian or Chinese blandishments or coercion. He argues for Washington first to shore up its own longstanding competitive advantages in technological innovation, finance, and entrepreneurship as a haven for ambitious immigrants and as a beacon of democracy. He calls domestic renewal a precondition for effective GPC, not a mere afterthought. Wyne also points to

America's clear post-World War II advantage in forging alliances and coalitions, observing that proper American Great Power strategy must rejuvenate existing alliances and forge new strategic partnerships. America, Wyne notes, will develop partnerships durable enough to withstand the challenges of long-term rivalry by inviting strategic partners to have a say in updating key elements of the global order, building a system better able to withstand the stresses of globalization while simultaneously blunting the actions of Russia and China that threaten world stability and peace.

As 2023 unfolds, the Biden administration is pursuing much of the agenda prescribed in *America's Great-Power Opportunity*. The Biden October 2022 National Security Strategy largely adopted the Trump administration's framing of GPC as a proper description of the new geostrategic reality. The Biden team also has championed domestic American renewal as a precursor for enhancing and expanding alliances and partnerships around the world that work to secure liberty, freedom, and peace while confronting coercive techniques and tactics practiced from Moscow and Beijing. In this sense, the United States already is approaching contemporary GPC as an opportunity, not just a challenge.

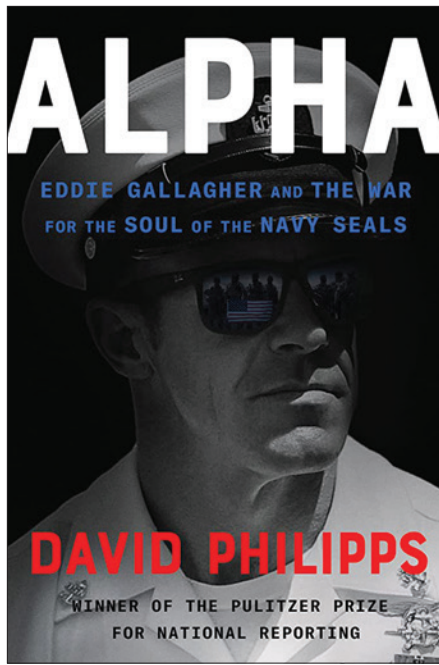
But the road ahead for America in this new era of GPC is far from smooth or certain. Historically, Great Power rivalries last for decades, not years. The costs, burdens, and challenges of day-to-day competition against powerful rivals often acting without moral or ethical constraints will be grinding for Americans. Moreover, the need to strike compromises with unsavory partners and allies will grate on the American polity. The risks from weariness and competition fatigue will be a persistent refrain—one already evident in early 2023 with calls by some vocal politicians to disengage from financial and material support of Ukraine in its just war against invading Great Power neighbor Russia.

Throughout its 246-year history, America's approach to foreign policy and international affairs arguably has been characterized best by University

of Pennsylvania political scientist Walter McDougall in his book *Promised Land, Crusader State* (Houghton Mifflin, 1997)—one of "exceptionalism." McDougall demonstrates that this populist foreign policy framework of exceptionalism has led Americans to a binary strategic approach that either rejects any direct engagement with messy GPC entanglements or pursues crusaderism-as-strategy where Americans engage globally with muscular unilateralism to project U.S. standards and ideals onto other countries. Neither of these traditional alternatives is particularly appropriate for the moment. Both Wyne and the Biden administration appear to understand the need to break from past American foreign policy proclivities, but can Americans be persuaded to come along?

America's Great-Power Opportunity thoughtfully appeals for a more nuanced American understanding of our new era of multi-state GPC and a mature foreign policy approach to it. Logical and appealing, Wyne's call for competitive maturity begs a crucial question: Is such maturity feasible given the American strategic tradition? We all must hope so. JFQ

Thomas F. Lynch III is a Distinguished Research Fellow in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.



Alpha: Eddie Gallagher and the War for the Soul of the Navy SEALs

By David Philipps

Crown, 2021

399 pp. \$24.49

ISBN: 9780593238387

Reviewed by Paula G. Thornhill

A *lpha* is a fast-paced, brilliantly written, and ultimately disturbing book about the health of the Navy SEAL community. Using the infamous Eddie Gallagher case for its core narrative, *Alpha* weaves together Gallagher's actions and the larger developments in Naval Special Warfare during the wars in Iraq and Afghanistan. The SEALs emerge from this era as a troubled organization, full of first-rate special operators willing to take on the toughest direct-action missions but largely devoid of a higher moral code to guide their actions and dismissive of any oversight beyond that of the insular world of special operations.

David Philipps approaches his topic with a keen reporter's eye. A Pulitzer Prize winner and *New York Times* correspondent, he meticulously pieces together the Gallagher story, starting with

how Gallagher overcame “bad karma” to build an aggressive, seemingly cohesive unit prior to deploying to Iraq. Once in theater, however, Gallagher malevolently used the unit to launch senseless attacks and kill innocent civilians. This steroid-dependent chief petty officer also rides roughshod over his platoon commander and assistant platoon commander throughout the deployment, denying the unit of any officer leadership and further undermining unit morale.

Once back from Iraq, some of the SEAL team members reflected on what happened and concluded that Gallagher had to be held accountable. This decision set into motion the subsequent investigation, trial, and eventual Presidential pardon that, at times, consumed not only the platoon and the SEALs but also the entire Navy.

Needless to say, *Alpha* is an uncomfortable read, bringing to light some troubling cultural issues in a loosely supervised, largely autonomous part of the U.S. military. By telling this story, it provides invaluable insights into how an insular culture can be built, sustained, and ultimately abused by those entrusted to protect it. Some SEALs argue that Philipps unfairly implies that the SEAL cultural problems are more profound and widespread than the community assesses. Even if this is the case, and readers must judge for themselves, he compels joint force members to think more holistically about the building, maintenance, and oversight of small, elite units. In particular, three major issues for the joint force to address emerge in *Alpha*.

First, what is the role of company grade officers in elite units? In *Alpha*, the SEAL platoon leader is physically strong, seemingly brave under fire, but devoid of moral courage. Gallagher's failure to exercise leadership allows him and his toxic culture to flourish. Where does responsibility rest for this moral failure? With the junior officer, the training, the SEAL culture he joined, or all the above? Understanding and addressing this leadership shortcoming is essential not only to the development of future SEAL officers but also to determining the extent to which they shape the organization they ostensibly lead.

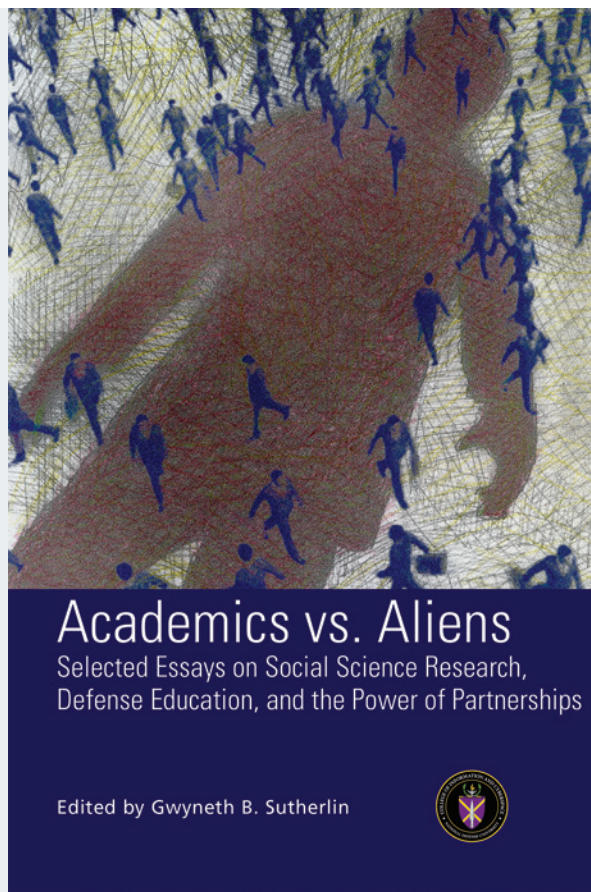
Second, closely tied to this leadership issue is a cultural one. Reading *Alpha*, we sense that SEALs are more akin to a professional sports team than a military unit—except kills, not goals, are the measure of the team's performance. This cultural nihilism belongs to the SEAL “pirate” subculture that dates to the Vietnam War. Pirates believe they are the true SEALs, who do the Nation's dirty work by rule-breaking, secrecy, and excessive killing. They are challenged at times by SEALs belonging to another, smaller subculture, the “boy scouts,” who believe they must operate under a code of law and order. Using Gallagher's case to highlight this tension, Philipps argues every SEAL must choose to belong to one subculture or the other; and since the 1970s, SEALs, including Gallagher, overwhelmingly have chosen the pirate culture. For the joint force, even discussing this construct is instructive. Some informal conversations with special operators indicate Philipps's characterization is on the mark. Others suggest that SEALs must simultaneously be pirates and boy scouts—a difficult task indeed. Thus, we must ask, where does, and should, the SEAL community's cultural epicenter rest, and what is the best way to nurture it?

Third, as a corollary, what are the SEALs doing to help young team members understand and develop moral courage to match their physical prowess? If a small fraction of the time devoted to rigorous physical training focused instead on this moral component, it could weaken the barrier between the pirate and boy scout subcultures. As important, it could better prepare young team members to deal with their own invisible wounds and help others do the same. If the SEALs, and special operators overall, want stronger organizational cultures, they need to pay heed to this moral dimension.

By flagging these issues, Philipps more than delivers to the joint force audience a well-written, infuriating account of Gallagher and a rogue SEAL platoon at war. Indeed, *Alpha* offers the reader a cautionary tale about how even the most elite units can lose their way when toxic culture, security classification, and lavish praise collectively undermine unit effectiveness

and accountability. Joint force leaders at all levels will finish this book powerfully reminded that high military effectiveness, healthy organizational culture, and leadership accountability are inextricably intertwined. Philipps did the joint force a huge service by creating such a vivid reminder of this crucial interrelationship. JFQ

Brigadier General Paula G. Thornhill, USAF (Ret.), is Associate Director of the Strategic Studies program in the School of Advanced International Studies at The Johns Hopkins University and author of *Demystifying the American Military: Institutions, Evolution, and Challenges Since 1789* (Naval Institute Press, 2019).



New from NDU Press

for the College of Information and Cyberspace

Academics vs. Aliens: Selected Essays on Social Science Research, Defense Education, and the Power of Partnerships

Edited by Gwyneth B. Sutherland

This edited volume shares the experiences of the first students and partners in the Minerva Defense Education Civilian University Research Partnership (DECUR) program. Their reflections offer a unique perspective on the collaborative approach for basic social science research. The National Defense University deliberately placed professional military education students at the center of the research design in partnership with technical experts and asked them to consider what role research can plan in national security and education. The approach challenged preconceived notions about academia, military, and government perspectives, leading to improved communication of priorities and knowledge as well as more relevant solutions to the topic of “Understanding Chinese Influence.”



Members of West Virginia National Guard and District of Columbia National Guard compete in the WV/DC 2023 Best Warrior Competition, April 21–23, 2023, at Camp Dawson, West Virginia (U.S. Army National Guard/Edwin L. Wriston)

Mission Assurance

Decisionmaking at the Speed of Relevance

By Ari Fisher

Thunderous was the sound of my sudden slip and fall in a tank motor pool that had become an ice-skating rink during this characteristic Polish winter. Turning around, the Army brigade commander generously attempted to soothe my embarrassment

Lieutenant Colonel Ari Fisher, USA, is the Chief of Headquarters Support Division, U.S. Indo-Pacific Command.

by stating he did the same thing in front of the commanding general a few days prior. On the clock to demonstrate port to fighting position posture, this rare staff officer excursion with the division deputy commanding general was to observe the brigade's readiness. While good staff work identified desirable metrics and accounted for equipment debarked from rail cars, and subordinate command operations centers

submitted daily personnel, training, and equipment readiness reports, the question remained: "When exactly is this brigade ready to fight?"

Later discussing that visit to the brigade's motor pool, our team of staff officers realized that despite the metrics and reporting, the deputy division commander was unable to make decisions at a relevant speed. He needed to more adequately "see" his command in time and



Army paratroopers assigned to 4th Battalion, 319th Airborne Field Artillery Regiment, fire M119A3 Howitzer during field artillery live fire exercise as part of exercise Bayonet Ready 22, at Joint Multinational Training Center, Grafenwoehr Training Area, Germany, October 25, 2021 (U.S. Army/John Yountz)

space. In an effort to refine understanding through daily dialogue, the brigade commander continued writing narratives to the deputy division commander. With the staff's metrics, they not only helped visualize the command in time and space but also described what the command could do within that time and space. For example, with an assembled 50 percent aggregated strength of the maneuver battalions, 33 percent strength of organic intelligence, surveillance, and reconnaissance (ISR) assets, and 50 percent strength of the sustainment battalion, the brigade could conduct security and reconnaissance for 48 hours—east of the line of departure—not to exceed the next phase line. ISR assets are focused forward and to the south flank with increased risk to support areas in the east as well as delayed opportunity to regenerate combat power. To this brigade commander,

he was always ready to fight. The only variance was relative to distance and duration. In this case, better decisions for the deputy division commander came from a valuation of the question: “What can I do right now?” He had to be able to diagnose his warfighting capacity, a function not only of what he fights with, but also how he fights.

In 2020, far from that Polish winter, on a sun-soaked hilltop overlooking Pearl Harbor, the COVID-19 pandemic had staff officers at U.S. Indo-Pacific Command (USINDOPACOM) asking similar questions relative to strategic warfighting readiness. After exhaustive planning groups and application of systems and processes as normal, it was clear that the combatant commander could not “see” what his command could do in time, space, or domain. More troubling, early on incubation periods of 5 to 10

days made it difficult to make decisions, allocate resources, or assume risk at a speed of relevance. As a staff, it was time to adapt. For the command's mission assurance (MA) team, the lessons planted in a Polish winter bore fruit in a Hawaiian summer. To support decisionmaking, the concept of MA needed to become pertinent to how a combatant command executes strategic warfighting—a whole-of-command critical capability perspective.

Relative to strategic warfighting, assuring warfighting performance must focus on command critical capabilities. Command critical capabilities designed for the competition continuum articulate how the command is currently fighting and will continue to fight at the simultaneous execution order of additional plans. These collectively applied actions, or the blocking and tackling of USINDOPACOM warfighting, needed



to be identified, performance measured, and risk mitigated. Opportunities, challenges, and pacing threats across the competition continuum and within this vast and diverse area of responsibility demand optimized decisionmaking. Heeding the call for a paradigm shift, this article explores why the existing Department of Defense (DOD) MA construct must evolve; the operational context in which MA is applicable; and how to identify, analyze, and manage risk to command critical capabilities.

Framing the Problem

Outmoded mission assurance myopia, which identifies and remedies vulnerabilities complementary to Defense Critical Infrastructure (DCI), typifies a construct that is overoptimized for the things we fight with at the expense of timely decisions that affect the way in which we fight. Constrained resources' vital role in assuring mission performance and *how we fight* will soon

outpace the DOD ability to prioritize and deliver them in time, space, and domain. This is primarily due to the inflexible nature of the existing DCI-focused MA construct. Furthermore, this antiquated approach excludes key areas and stakeholders, beyond DCI, that can illuminate strategic critical weaknesses—accumulated emerging vulnerabilities, requirements, and applied mitigation affecting mission performance.¹ Interestingly, the DOD 2012 Mission Assurance Strategy established a solid intellectual foundation.² However, in application, the 2022 DOD MA instruction implements a model that depends on latent off-the-shelf operational plans offering only peace or war advantages.³ In fact, when reviewing what manuals and programs it incorporates and replaces, this instruction is DCI and asset protection by another name. Today's rapidly adaptive gray zone and unrestricted warfare models render this method stale, which will invariably result in decisions and resources arriving too late. Consequently, DOD Global Security efforts must coalesce Service and combatant command proactive approaches to maintaining MA within critical defense mission areas and remodel the process by which senior leaders make risk-informed strategic decisions at the speed of relevance.

In today's globally integrated, competitive, joint, and multinational operating environment, the current and simultaneous execution of multiple plans demands a thorough analysis of critical capabilities, which is *how we fight*. This analysis must assess performance where it intersects in time, space, and domain to improve understanding and identify risk not previously revealed during the assessment of a singular plan. Unrestricted warfare, as envisioned by Qiao Liang and Wan Xiangsui, is a prime example.⁴ These authors describe warfare as fully inclusive, playing out in seas and contested territorial waters as well as in social, economic, and information spaces. Since a nation's navy, coast guard, maritime militia, and state-sponsored fishing collective may only differ in degree, characteristically then, naval activity just below armed

conflict in Northeast Asia manifests differently than naval and maritime cooperation in South Asia. Furthermore, global common and market integration means that what happens in one region or theater will affect another.

It is in this competitive continuum where MA can enable decisionmaking and give significance to emerging operational and strategic requirements in high demand, and DOD serves as global integrator. As such, MA is a “whole of command” critical capability perspective, encompassing critical requirements—essential conditions, resources, and means—to enable mission execution within a given theater. Therefore, we achieve MA results from the identification, analysis, and management of risk affecting critical capabilities. This is *crucial* for the command to adaptively transition across the competition continuum.

Strategic Warfighting Context

DOD must recast mission assurance as an integral method to strategic warfighter in which the Joint Concept for Integrated Campaigning provides the appropriate grammar. MA can optimize leader decisionmaking to deliver risk-informed performance at the speed of relevance. Maximizing critical capability performance aims to provide and sustain resources with operational reach across the competition continuum while preventing potential culminating points to current or future military objectives. Differing from a binary peace or war offering across operational, contingency, and functional plans, the competition continuum provides an alternative logic where various states of relationships can exist concurrently within an operating environment and facilitate required civil-military dialogue. Relative to Great Power competition, critical capabilities—organized along the competition continuum—enable decisions to apply risk-informed performance at the time, space, and domain of consequence.⁵ Within this competition continuum, command critical capabilities dictate

operational need by generating critical requirements and demand obligation of limited resources from joint, interagency, and multinational partners.

Critical Capabilities for the Competition Continuum

The competition continuum—cooperation, competition below armed conflict, and armed conflict—provides an effective frame to apply the command's critical capabilities. Critical capabilities are a *primary ability* essential to the accomplishment of specified or assumed objectives.⁶ In practice, at USINDOPACOM, a critical capability is an action to apply *essential means* across the competition continuum to execute operations, activities, and investments (OAIs) and complete objectives organized along lines of effort (LOEs) to achieve regional or strategic goals.⁷ These actions comprise defeat, stability, or competition mechanisms as they help align military and nonmilitary activities.⁸

Aligning our critical capabilities as mechanisms creates a common understanding and amplifies emerging critical requirements to the joint, interagency, and multinational (JIM) coalition by emphasizing operational impact or risk to current and future OAIs.⁹ Examples of critical capabilities with these mechanisms could be to:

- destroy adversary decisive points through joint forcible entry (defeat mechanism)
- create distributed power projection platforms (competition mechanism)
- preserve combat power regeneration areas (competition mechanism)
- disintegrate through lethal and non-lethal fires (defeat mechanism)
- isolate adversary command and control (C2) nodes through electromagnetic, cyber, and space effects (defeat mechanism)
- influence ally, partner, and host-nation populations (stability mechanism)
- position irregular warfare competency in adversary support areas (competition mechanism).

Essential conditions, resources, or means comprise the tangible things requisite for critical capabilities to be fully operational. Those essential conditions, resources, and means—often referenced as capabilities, activities, assets, people, infrastructure, or effects—are, by definition, *critical requirements*.¹⁰ As such, critical requirements in their many forms enable the joint force commander to perform critical capabilities.¹¹

Critical Requirements

Critical requirements are frequently named “items” or “systems.” When named, these items add specificity to a general means or resource.¹² As a result, specific critical requirement availability often reflects the readiness of the item performing or delivering the capabilities, activities, assets, people, infrastructure, or effects. In this setting, we commonly refer to the nomenclature of specific sensors, material handling equipment, logistics storage, communication or satellite devices, warfighting platforms, weapons systems, ordnance types, military occupational specialties, or authorities. This specificity is noteworthy when those items are synonymous with a requirement gap or are in short supply and the command must attain them instead of another combatant command to assure operational effectiveness of a critical capability. Examples of critical requirements, in italics, with their associated joint function and what the critical capability mechanisms could be, include:

- project *F-35s* to achieve air superiority (fires, destroy)
- protect *command, control, computers, communications, intelligence* with *defensive cyber effects* (C2, destroy)
- deploy *200 Twenty-Foot Equivalent Units of ammunition* through *SPOD X-Ray* (sustainment, create)
- provide *fuel* to support *air sortie regeneration* (sustainment, create)
- protect *air/seaport of embarkation, air/seaport of debarkation*, and power projection from *improvised threats* (protection, create)
- establish *logistics support areas* (sustainment, preserve)

- employ *joint electromagnetic spectrum operations activities* (fires, disintegrate)
- disrupt adversary C2 with *offensive space* and *cyber effects* (C2, defeat)
- deploy *medical specialists* and *personal protective equipment* to support foreign humanitarian assistance (information, influence)
- conduct *foreign internal defense* (intelligence, position).

The articulation of critical requirements with their associated critical capabilities highlights the context and operational need of those capabilities, activities, assets, people, infrastructure, or effects. For example, limited or degraded Terminal High Altitude Air Defense (critical requirement) availability or readiness necessitates more of that resource or one that can deliver the same protection effect. Without it, the command is less able to preserve combat reconstitution areas (critical capability), resulting in increased risk to mission.

Joint functions provide a frame to identify command critical requirements. Joint functions group related capabilities, activities, assets, people, infrastructure, or effects to assist joint force commanders in synchronizing, integrating, and directing joint operations.¹³ Any discussion of incorporating critical requirements as essential means and conditions to critical capabilities must be synchronized, integrated, and directed through the joint functions. While this occurs most notably as OAIs, their derived operational impact or risk is fundamental not only to MA but also to supporting realistic and real-time commander visualization of what is possible given current and available critical capability and joint function performance.

Critical Capability Identification

As a doctrinal method, analysis of critical factors focuses on critical capabilities and requirements. This analysis can create a nested and shared understanding by linking the vulnerabilities of our critical requirements to critical capabilities and illuminating cross-functional strategic warfighting



Marines with 3rd Reconnaissance Battalion jump from KC-130J Super Hercules assigned to Marine Aerial Refueler Transport Squadron 152, Marine Aircraft Wing 36, during military free fall and low-level static line parachute operations over Ie Shima, Okinawa, Japan, May 16, 2023 (U.S. Marine Corps/Michael Taggart)

risk. What results is an improved sight picture to support decisionmaking and the allocation of resources.¹⁴ In practice, at USINDOPACOM and across the competition continuum, a critical capability is an action applying critical requirements to complete objectives organized along LOEs and to achieve strategic goals. Accordingly, critical capability identification consists of a thorough review of the USINDOPACOM Theater Campaign Plan (TCP),

the Decision Deterrence Framework, and operational plans.

The USINDOPACOM TCP articulates strategy during cooperation and competition. Four LOEs form the framing model to achieve regional campaign or strategic objectives below armed conflict. By analyzing these LOEs and their associated intermediate objectives, we can distill specific actions that are crucial to applying essential means, or those capabilities, activities, assets,

people, infrastructure, and effects. They materialize as operations, activities, or investments to gain relative all domain positional advantage. Therefore, as defeat, stability, or competition mechanisms, USINDOPACOM critical capabilities contextualize OAI across an area of responsibility that spans five distinct regions and 52 percent of the globe where varying degrees of relationships exist. As a result, command critical capabilities must facilitate employment of flexible options.



Air Force Captain Orr "Recoil" Genish, 37th Bomb Squadron weapons systems officer, uses land mobile radio as he watches B-1B Lancer land in support of Bomber Task Force mission at Naval Support Facility Diego Garcia, October 17, 2021 (U.S. Air Force/Hannah Malone)

The USINDOPACOM Decision Deterrence Framework delivers flexible OAI options within the cooperation and competition continuums but below armed conflict. Through analysis enabled by this framework, we can ensure critical capabilities support the exploration of deterrence options across time, space, and domain. Subsequently, these flexible options drive readiness awareness of critical requirements—those capabilities, activities, assets, people, infrastructure, or effects—that the command has or will need to win without fighting. Should deterrence fail, as defeat, stability, or competition mechanisms, USINDOPACOM critical capabilities in application permit

the adaptive transition into operational plan's LOEs to engage in armed conflict.

Operational plans articulate how we intend to engage in armed conflict with potential adversaries. Command critical capability performance from competition below armed conflict will frame—in time, space, and domain—the command's initial warfighting potential to deliver effects. As a result, we organize command critical capabilities within the joint functions. This organization supports the synchronization and integration of OAIs and supports the dialogue encompassing critical requirements as essential means and conditions to critical capabilities as crucial enablers in armed conflict. Therefore, not only in

armed conflict but also across the competition continuum, the command must objectively determine critical capability performance potential or degradation.

Critical Capability Analysis

Critical capability analysis evaluates performance potential or degradation to support leader decisionmaking to allocate constrained resources and assume prudent risk. The command's ability to see itself through the health of its critical capabilities hedges against adversary OAIs to create or exploit vulnerabilities.¹⁵ Defense programs and activities (for example, antiterrorism, ballistic missile defense, and

defensive cyber operations) are the primary sources of aggregating a total performance score for our command critical capabilities. Taking these diverse metrics and achieving a currency conversion to performance of critical capability and joint function by region is a matter of integrating a standard risk framework from the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3105.01A, *Joint Risk Analysis Methodology*.¹⁶

Aggregating program readiness metrics is the principal method in evaluating critical capability performance. The joint functions contain associated missions, tasks, or processes to organize those critical requirements or essential capabilities and activities, all of which have program or activity owners. These offices of primary responsibility (OPRs) analyze through their own program measures to determine the readiness or effectiveness of capabilities, activities, assets, people, infrastructure, or effects as critical requirements. They then associate each measure to the critical capabilities they affect. While it is likely that each OPR measures its respective programs or critical requirements using differing standards, when we aggregate performance metrics across the community of interest, we will integrate those scores using a standard methodology to yield a total score. For this integration, we use CJCSM 3105.01A as our framework. As a result of this integration, we can place these OPR program metrics in context of one another, relative to a critical capability removing gaps between existing stovepiped readiness reporting methods.

Achieving a currency conversion for program measures is vital to achieving a performance score for each critical capability and joint function by region to support rapid and adaptive transitions within the competition continuum. For each program OPR, we inquire along two axes: impact and consequence. Impact is a function of assessed operational reach, bounded by distance and duration, a critical capability is performing. Consequence is the assessed probability that the OPR's current program score will result in a culminating point. We then average these

assessed probabilities and repeat the process for all five regions within the theater. Aggregation of these metrics occurs for each critical capability and then again by joint function regionally. This process results in risk-informed performance to support decisionmaking.

Critical Capability Risk Management

Maximizing critical capability performance aims to provide and sustain resources with operational reach while preventing potential culminating points to current or future military objectives. As a result, through analysis of risk drivers, MA risk management focuses on problem-framing, risk assessment, and risk characterization while enabling risk communication within the joint risk analysis framework.¹⁷

Problem-framing and risk assessment are a direct result of critical capability analysis and the aggregation of performance metrics. By assessing performance potential along the same probability and consequence scale, we can determine low, medium, significant, or high degree of performance degradation. Subsequently, the total performance score paired with risk to force, mission, or strategy builds an initial risk problem frame. Scores aggregating by critical capability and then again by joint function give quantitative significance to the operational need for constrained resources necessary to mitigate risk within the JIM coalition.

Risk communication occurs through the boards, bureaus, centers, cells, working group (B2C2WG) process to support decisionmaking by informing strategic estimates to improve the commander's understanding of critical capability performance. The USINDOPACOM MA Division (J34) in the Operations Directorate (J3) serves as a joint function integrator through the MA Working Group (MAWG) to frame problems and facilitate initial risk assessment and characterization. Functionally and procedurally, this provides a shared MA community estimate as an input into other command processes and B2C2WGs. For instance, this assessment and characterization helps inform initial running estimates

that the Operational Planning Group needs for the employment of critical requirements relative to the deterrence decision framework to execute OAI. In another example, this assessment and characterization helps inform the Joint Planning Group of emerging gaps or requirements ahead of transition within the competition continuum or phase of operation. This risk communication eventually elevates to the validation and steering boards for consideration as the commander makes decisions, allocates resources, or assumes residual risk. For specific actions taken to address identified risk drivers, the MAWG directly feeds the Mission Assurance Control Board, which is chaired by the command's chief of staff who in this forum synchronizes and provides discipline across the staff. Additionally, for mitigating actions on risk drivers that come from outside the command, the chief of staff may apply emphasis and urgency up to the Joint Staff and DOD.

Summary Recommendations

Adversaries seeking temporary or sustained overmatch may only need to deny our ability to attain all-domain positions of advantage. As a result, the aperture for critical weaknesses is far wider and more networked than what DOD considers a DCI-critical vulnerability and spans potential cross-functional fissures that can exist between commands and Services. This is especially true in today's all-domain strategic warfight where assuring mission performance extends across individual geographic (GCC) and functional (FCC) combatant command authorities and includes critical requirements, which may be supporting other strategic and global efforts.

Consider the Russia-Ukraine war. In the first 4 weeks of the war, the United States supplied Ukraine with approximately 4,600 Javelin antitank weapons of around 8,900 procured in a decade.¹⁸ While doing this must satisfy a near-term requirement, it must be done in context to the critical capability performance of all GCCs. For instance, how does this allocation of resources in Europe

affect USINDOPACOM's ability to position irregular warfare competency? Furthermore, this case illuminates the challenge DOD retains in allocating resources to an active threat in Europe to the pacing of longer term challenges in the Pacific region.¹⁹ For example, how does subsequent funding support to Ukraine affect the Pacific Deterrence Initiative—an initiative that wants to apply more focus on fundamental critical capabilities?²⁰ Therefore, DOD Global Security efforts must coalesce Service and combatant command proactive approaches to maintaining MA within critical defense mission areas and remodel the process in which senior leaders can make risk-informed strategic decisions at the speed of relevance.

Adapting USINDOPACOM's MA concept to other combatant commands supports global security integration. This can occur by DOD directing GCCs and FCCs to identify command critical capabilities and adopting USINDOPACOM's performance analytical model. This effort would require revision of DOD Instruction 3020.45, *Mission Assurance Construct*, shifting the focus from defense critical infrastructure onto critical capabilities across the competition continuum and the integration of programs and activities within context of their joint and theater warfighting application to defense critical mission areas. Nesting GCC and FCC command critical capabilities within defense mission areas enables a global visualization of the DOD strategic warfighting performance in real time, space, and domain. The added specificity and clarity will yield better global strategic risk decisions.

Remodeling our MA B2C2WG process must continue to break down silos and increase the opportunity for senior leaders to make risk-informed decisions. At the command levels, MA helps to remove stovepipes by placing different programs and activities in context with one another relative to a critical capability the command must execute with operational reach for mission success across the competition continuum. Similarly, DOD must modify existing steering groups to address critical weaknesses

and vulnerabilities not only related to combatant command and Service critical capabilities but also among these commands. In today's globally integrated environment, no command will compete below armed conflict or engage in armed conflict alone. This modification and strategic focus across GCCs and FCCs will support relevant risk dialogue at a speed that allocates critical requirements in time, space, and domain ahead of need. Currently, existing inflexible and singularly DCI-focused decision cycles that span months fail to keep pace with the increasing speed of strategic competition and only fractionally address how pacing threats view our critical weaknesses.

Shedding inflexible and outmoded practices to gain strategic flexibility requires a global MA model that identifies, analyzes, and facilitates risk management of critical capabilities crucial to strategic warfighting and adaptive transition within the competition continuum. Global security's ability to remodel the decisionmaking process and coalesce Service and combatant command proactive approaches to maintaining mission assurance within critical defense mission areas will demonstrate MA as an integral method to strategic warfighting. This important paradigm shift, which is inclusive of strategic warfighting critical weaknesses beyond DCI, is the solution to assure mission performance with operational reach. By dually directing effort on our decisionmaking process focused on how we fight, our methods of strategic warfighting, DOD has more opportunity. Through the delivery of constrained resources enabling commands at echelon to seize initiative and retain positional advantage in an all-domain strategic warfight, not only will we keep pace, but we will also set tempo and dictate terms. JFQ

Notes

¹ Jack D. Kem, *Planning for Action: Campaign Concepts and Tools* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2012), 186, <https://apps.dtic.mil/sti/pdfs/ADA564371.pdf>.

² *Mission Assurance Strategy* (Washington, DC: Department of Defense [DOD],

April 2012), https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.

³ DOD Instruction 3020.45, *Mission Assurance Construct* (Washington, DC: DOD, August 14, 2018, Change 1, May 2, 2022), <https://www.esd.whs.mil/Portals/54/Documents/DD/is-suances/dodi/302045p.pdf?ver=4Jg-492hgFA2cDsUPGmREA%3D%3D>.

⁴ Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: Two Air Force Senior Colonels on Scenarios for War and the Operational Art in an Era of Globalization* (Beijing: People's Liberation Army Literature and Arts Publishing House, 1999).

⁵ *Joint Concept for Integrated Campaigning* (Washington, DC: The Joint Staff, March 16, 2018), vi, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.

⁶ Joint Publication (JP) 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), IV-25, https://irp.fas.org/doddir/dod/jp5_0.pdf.

⁷ Kem, *Planning for Action*, 183.

⁸ *Joint Concept for Integrated Campaigning*, 6.

⁹ *Ibid.*, 12.

¹⁰ JP 5-0, IV-25.

¹¹ Kem, *Planning for Action*, 185.

¹² *Ibid.*, 200.

¹³ JP 5-0, III-1.

¹⁴ Joint Forces Staff College (JFSC) Publication 1, *The Joint Staff Officer's Guide 2000* (Washington, DC: JFSC, 2000), 3-55, <https://apps.dtic.mil/sti/pdfs/ADA403118.pdf>.

¹⁵ *Ibid.*, 3-57.

¹⁶ Chairman of the Joint Chiefs of Staff Manual, *Joint Risk Analysis Methodology* (Washington, DC: The Joint Staff, October 12, 2021), [https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM 3105.01A.pdf?ver=y3cH4s5UNyqJAXwxAYCL5Q%3D%3D](https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%203105.01A.pdf?ver=y3cH4s5UNyqJAXwxAYCL5Q%3D%3D).

¹⁷ *Ibid.*, B-2.

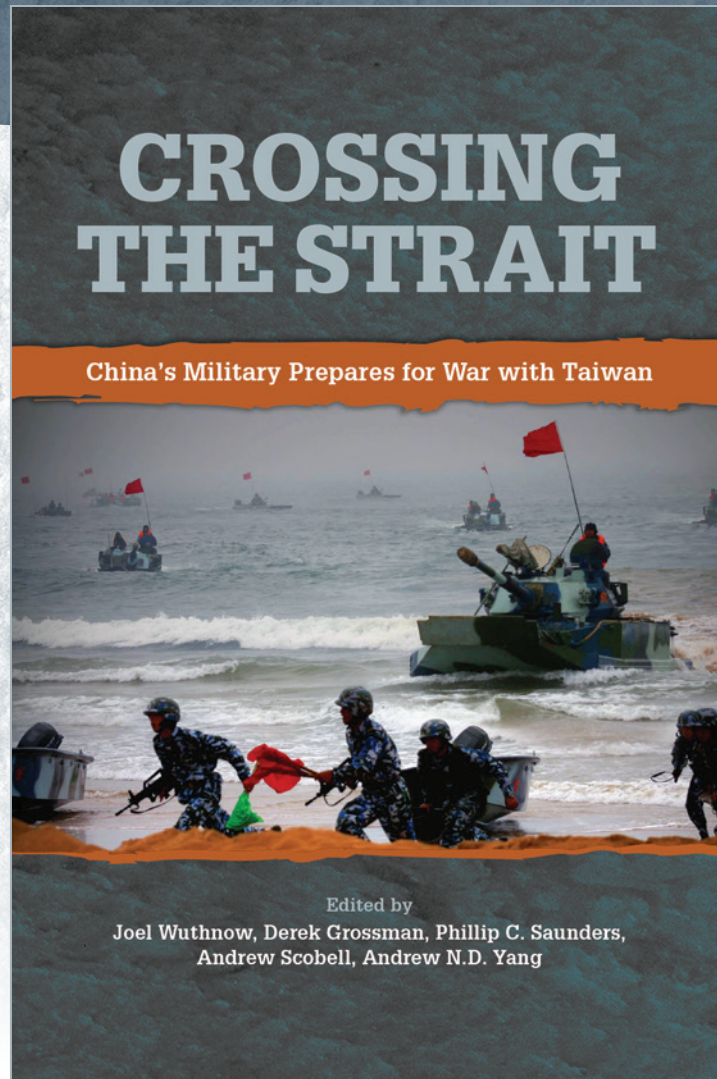
¹⁸ John Schaus, "Saint Javelin of Limited Supply," *Center for Strategic and International Studies*, March 28, 2022, <https://www.csis.org/analysis/saint-javelin-limited-supply>.

¹⁹ David Sacks, "Don't Pivot From the Pivot to Asia," *Council on Foreign Relations*, March 21, 2022, <https://www.cfr.org/blog/dont-pivot-pivot-asia>.

²⁰ Dustin Walker, "Pacific Deterrence Initiative: A Look at Funding in the New Defense Bill, and What Must Happen Now," *Defense News*, December 15, 2021, <https://www.defensenews.com/opinion/commentary/2021/12/15/pacific-deterrence-initiative-a-look-at-funding-in-the-new-defense-bill-and-what-must-happen-now/>.

New from NDU Press


for the Center for the Study of Chinese Military Affairs




Both the U.S. and Chinese militaries are increasingly focused on a possible confrontation over Taiwan. China regards the island as an integral part of its territory and is building military capabilities to deter Taiwan independence and compel Taiwan to accept unification. Based on original research by leading international experts, *Crossing the Strait: China's Military Prepares for War with Taiwan* explores the political and military context of cross-strait relations, with a focus on understanding the Chinese decision calculus about using force, the capabilities the People's Liberation Army would bring to the fight, and what Taiwan can do to defend itself.

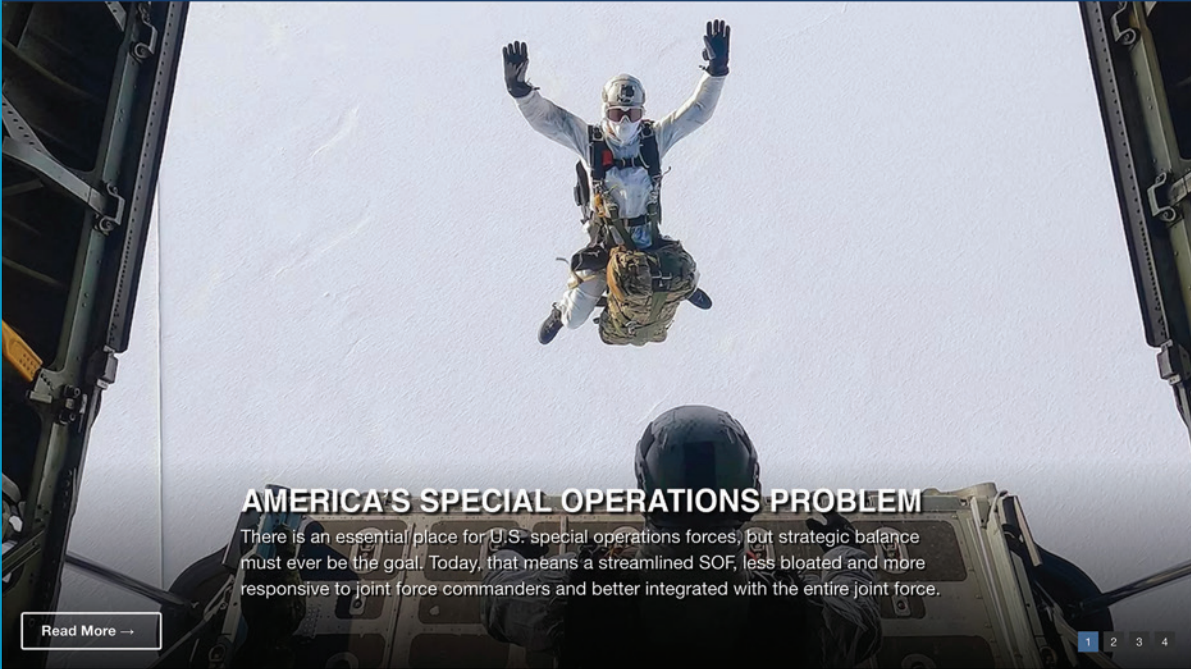
Check Out NDU Press Online!

Each year more than 1.5 million people visit the NDU Press Web site from around the world to discover the issues the joint force is experiencing in current policy, security, and warfighting arenas.

**NATIONAL DEFENSE UNIVERSITY PRESS**
THE PREMIER PROFESSIONAL MILITARY AND ACADEMIC PUBLISHING HOUSE

Search NDU Press 

[HOME](#) [ABOUT](#) [JFQ](#) [PRISM](#) [PUBLICATIONS](#) [SUBMIT A MANUSCRIPT](#) [CONTACT](#)




AMERICA'S SPECIAL OPERATIONS PROBLEM


There is an essential place for U.S. special operations forces, but strategic balance must ever be the goal. Today, that means a streamlined SOF, less bloated and more responsive to joint force commanders and better integrated with the entire joint force.

[Read More →](#)


The premier professional military and academic publishing house of the National Defense University




PRISM VOL. 10, NO. 1 | SEPT. 30, 2022
The 21st Century's Great Military Rivalry
Graham Allison and Jonah Glick-Unterman



JOINT FORCE QUARTERLY 108 | JAN. 16, 2023
Choosing Your Problems
Michael A. Baker



PRISM VOL. 10, NO. 1 | SEPT. 30, 2022
Panda Power? Chinese Soft Power in the Era of COVID-19
Amit Gupta



JOINT FORCE QUARTERLY 108 | JAN. 18, 2023
America Must Engage in the Fight for Strategic Cognitive Terrain
Daniel S. Hall

You can also find us on:



Twitter



Facebook

JFQ

JOINT FORCE QUARTERLY

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

