



JFQ

Joint Force Quarterly

Issue 109, 2nd Quarter 2023

Black Soldiers and the Promise of America

Integrating the Private Sector into
U.S. Cyber Strategy

When Dragons Watch Bears

Joint Force Quarterly

Founded in 1993 • Vol. 109, 2nd 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

Shira Klapper

Caroline Schweiter

Book Review Editor

Brett Swaney

Designer

Jamie Harvey, John Mitrione,
U.S. Government Publishing Office

Advisory Committee

Lt Gen Dagvin R.M. Anderson, USAF/The Joint Staff; RADM Shoshana S. Chatfield, USN/U.S. Naval War College; BG Joy L. Curriera, USA/Dwight D. Eisenhower School for National Security and Resource Strategy; Brig Gen William C. Freeman, USAF/Air War College; Col Lee G. Gentile, Jr., USAF/Air Command and Staff College; MG David C. Hill, USA/U.S. Army War College; Ambassador (Ret.) Greta C. Holtz/College of International Security Affairs; Brig Gen Jeffrey H. Hurlbert, USAF/National War College; Cassandra C. Lewis, Ph.D./College of Information and Cyberspace; LTG Theodore D. Martin, USA/U.S. Army Command and General Staff College; BG Voris McBurnette, USA/Joint Forces Staff College; LTG James J. Mingus, USA/The Joint Staff; 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/Eisenhower School; Eliot A. Cohen/The Johns Hopkins University; Aaron L. Friedberg/Princeton University; Bryon Greenwald/National Defense University; COL James E. Hayes, USA/National War College; Douglas N. Hime/Naval War College; Col Eric M. Murphy, USAF/Eisenhower School; Paul J. Springer/Air Command and Staff College; Bert B. Tussing/U.S. Army War College

Cover 2 images (top to bottom): Senior Airman Theresa Braak, 436th Security Forces Squadron military working dog handler, and military working dog Sam negotiate window obstacle, October 8, 2020, at Dover Air Force Base, Delaware (U.S. Air Force/Mauricio Campino); Marine Corps Lance Corporal Manny, Marine Corps Recruit Depot San Diego mascot named after Sergeant Johnny R. Manuelito, one of original 29 Navajo Code Talkers, leads Charlie Company, 1st Recruit Training Battalion, in log drills alongside Senior Drill Instructor Sergeant Jarred A. Sagadraca, December 13, 2021 (U.S. Marine Corps/Grace J. Kindred); Ensign Sydney Hughes holds dog brought on board USS *George H.W. Bush* by Mutts With a Mission, July 13, 2022, Norfolk, Virginia (U.S. Navy/Novalee Manzella)



In This Issue

Forum

- 2 Executive Summary
- 4 A More Perfect Union: Black Soldiers and the Promise of America
By John Nagl and Charles D. Allen
- 14 Intermediate Force Capabilities: Nonlethal Weapons and Related Military Capabilities
By Sara McGrath
- 25 The New "Cyber" Space Race: Integrating the Private Sector Into U.S. Cyber Strategy
By Natalie R. Alen, Gregory M. Eaton, and Jaime L. Stieler

JPME Today

- 33 General George Washington: First in War, First in Peace, First in National Security Strategy
By David C. Arnold
- 41 Cyber Deterrence Is Dead! Long Live "Integrated Deterrence"!
By James Van de Velde

Commentary

- 51 A Mission Assurance Assessment of Threats to Missions and Force Protection Planning
By Michael J. Borders, Jr., and Miller Carbaugh
- 57 Napoleon Revisited
By George DiMichele

Features

- 63 When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force
By Christopher H. Chin, Nicholas P. Schaeffer, Christopher J. Parker, and Joseph O. Janke



About the Cover

Squad leader with U.S. Army's Second Squadron, 2nd Cavalry Regiment, shouts orders to his Soldiers during blank-fire exercise at Smârdan Training Area, in Romania, March 8, 2022 (NATO)

- 74 Mind the Gap: Space Resiliency Advantages of High-Altitude Capabilities
By Benjamin Staats

Recall

- 85 Echoes of the Past: The Burma Campaign and Future Operational Design in the Indo-Pacific Region
By Shane Williams, John Green, Richard Kovsky, and Edwin Sumantha

Book Reviews

- 94 Leadership Decapitation
Reviewed by Larry D. Miller
- 95 Resourcing the National Security Enterprise
Reviewed by Stephan Pikner
- 96 Cyber Persistence Theory
Reviewed by Stafford A. Ward

Doctrine

- 98 A Framework for Mission Analysis in the Space Planning Process
By Nicholas R. Shaw

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

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

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

Copyright Notice

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

Submissions and Communications

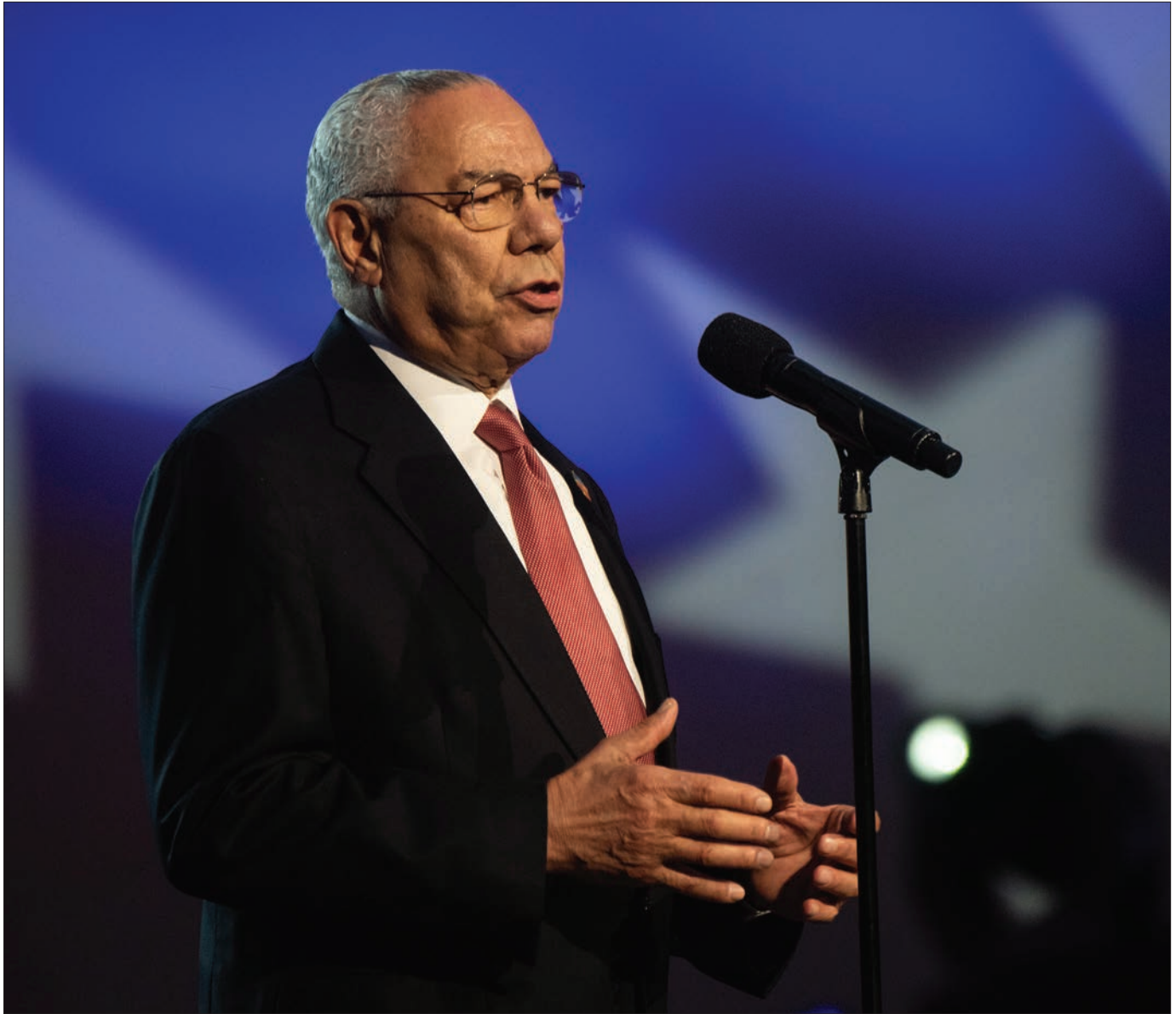
JFQ welcomes submission of scholarly, independent research from members of the Armed Forces, security policymakers and shapers, defense analysts, academic specialists, and civilians from the United States and abroad. Submit articles for consideration to ScholarOne, available at <https://mc04.manuscriptcentral.com/ndupress>,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

Editor, *Joint Force Quarterly*

NDU Press
300 Fifth Avenue (Building 62, Suite 212)
Fort Lesley J. McNair
Washington, DC 20319

Telephone: (202) 685-4220/DSN 325
Email: JFQ1@ndu.edu
JFQ online: ndupress.ndu.edu/jfq

2nd Quarter, April 2023
ISSN 1070-0692



General Colin Powell, former Secretary of State and 12th Chairman of the Joint Chiefs of Staff, speaks during National Memorial Day Concert on West Lawn of Capitol, Washington, DC, May 27, 2018 (DOD/James K. McCann)

Executive Summary

One of the enduring topics of any military person's—or anyone's—life is encountering leadership, whether good, bad, or in between. I recently reread Colin Powell's last book, *It Worked for Me: In Life and Leadership*. Just past the 20th anniversary of the start of the Iraq

War, I was particularly drawn to the chapter covering his 2003 speech at the United Nations on Saddam Hussein's alleged biowarfare capabilities. Powell was a very effective speaker who knew how the U.S. intelligence system worked and, despite its flaws, on that day trusted what he was told. As our

nation's leading diplomat, drawing on his military understanding of international affairs and national security strategy (he was a National War College graduate), he did what he saw as his duty. His words were powerful and persuasive. But as we all know now, they were based on flawed information.

What is remarkable now is his willingness, well before he died, to reflect on that time and openly admit his regret. Having studied military history my entire adult life, I know of few similar public admissions. It takes a certain amount of personal courage to accept responsibility for being wrong. Leaders are often confronted with their weaknesses, at times very publicly, and I submit that how they set the example in such situations is key to knowing whether one should follow them.

Revisiting Powell's thinking led to my rediscovery of another leadership expert, Jim Collins of *Good to Great* fame. Collins also wrote (with Jerry I. Porras) a book called *Built to Last*, in which he describes five levels of visionary leadership. Collins believes that the very best visionary leaders have an "X factor"—humility. These are driven people, and their drive is focused on something other than themselves. Collins believes these leaders live and act in a spirit of service both to others and to the goals they seek to achieve, ultimately achieving success not as individuals but as part of groups, giving credit to everyone involved. Anyone who has been in the military knows what it feels like to follow such leaders.

From Harry Truman's executive order to integrate the military racially and the Women's Armed Services Integration Act, both in 1948, to the removal of the combat exclusion of women just 10 years ago, the joint force has slowly adapted to a broader range of people serving and leading. Eighty years ago, the military's segregated units and combat exclusion policies reflected the country as it was then. The nation has constantly evolved since. But the challenges of sustaining and building on its progress remain.

From this chair, I am tracking the integration arc of the joint force, and we have all seen the advances minorities and women have made. But issues that are likely systemic—and therefore requiring systemic changes—persist, especially in fully integrating women into the force and in recruiting and retention. In addition, rates of criminal activity such as sexual harassment and assault against women and men are rising. Another

disturbing and persistent issue is military member and family member suicide.

I offer these thoughts to stimulate your thinking on where the joint force needs to be in the years ahead. Technology is important, but it is not the answer to issues of human nature or culture. Effective leadership must be achieved through training, education, enforcement of standards, effective and appropriate promotion policies, and focusing on respect for everyone who serves. As you experience success in your own lives, be sure to lead with enough humility to help those around you share in that success.

In this issue's Forum, we connect our very human past with the increasingly technological present and future of the joint force. First up, we have two of *JFQ*'s alumni, the U.S. Army War College's John Nagl and Charles Allen, who provide an important review of the rise of Black Soldiers in the Army. In investigating ways the military can best add capability without taking lives in the battlespace, Sara McGrath updates us on nonlethal weapons and similar military capabilities. Adding to the already significant and valuable discussions in these pages on cyber issues, Natalie Alen, Gregory Eaton, and Jaime Stieler provide some thoughtful insights on how the joint force can partner with industry in what they term the "new 'cyber' space race."

Our JPME Today section returns to this issue of *JFQ* with two contributions from the faculty here at the National Defense University. David Arnold, of the National War College, presents his case for how George Washington provided the Nation with its first national security strategy. And, with the concept of integrated deterrence now front and center in our defense policy, James Van de Velde, of the Dwight D. Eisenhower School of National Security and Resource Strategy, argues that previous approaches to cyber deterrence are now "dead."

Offering a wide-ranging set of Commentary articles, this issue takes you from today's threat-based planning to looking back at a certain European warrior-king. Suggesting that our present institutional views have underappreciated

the growing number of threats to the deployability of the joint force, Michael Borders, Jr., and Miller Carbaugh examine areas of concern and offer a framework for taking them into account. Seeing parallels in present-day Great Power competition to the world that gave rise to Europe's most famous emperor, George DiMichele recommends that we investigate the roots of Napoleon's successes.

In Features, you will find two very current pieces that tackle operational issues in multiple domains. The team of Christopher Chin, Nicholas Schaeffer, Christopher Parker, and Joseph Janke describes developments in information warfare with a focus on China and Russia and offers some very interesting recommendations. Looking to "near space," Benjamin Staats sees a number of opportunities for operating at elevations above where jet fighters were during the recent engagements with Chinese balloon flights over North American airspace.

Our Recall section brings us a look back at the Burma campaign of World War II. Shane Williams, John Green, Richard Kovsky, and Edwin Sumantha suggest that lessons from this campaign include the counterbalancing of cutting-edge technology with an opponent's mass and ability to persist. (One might glean a similar lesson from today's Russian war on Ukraine.) In Doctrine, Nicholas Shaw presents an impressive method for developing mission analysis for outer space plans. And as usual, we include three very useful book reviews to guide your professional development reading, along with the latest in Joint Doctrine. Insiders tell me we are likely to see a very big development in that area this summer.

As always, we are looking forward to what you have to say on leadership, on the transformation of today's world, and especially on where the joint force is headed and how to make sure it is ready to meet and succeed against the challenges ahead. *JFQ*

—William T. Eliason,
Editor in Chief

Buffalo Soldiers of 25th Infantry, some wearing buffalo robes, Fort Keogh, Montana, 1890 (Library of Congress)



A More Perfect Union

Black Soldiers and the Promise of America

By John Nagl and Charles D. Allen

Well into the third decade of the 21st century, the U.S. military is reassessing its

Lieutenant Colonel John A. Nagl, USA (Ret.), Ph.D., is Associate Professor of Warfighting Studies at the U.S. Army War College (USAWC). Colonel Charles D. Allen, USA (Ret.), is Professor of Leadership and Cultural Studies at USAWC.

connection to the society that it is chartered to protect and serve. While it is easy to declare and embrace the mission to fight and win the Nation's wars, it is more challenging to forge and sustain an institution that lives its espoused values and holds its members accountable for the principles put forth in its founding documents. In 1775, American colonists protested that

their rights as British citizens were not protected and subsequently established the fledgling Continental Army. A year later, the Declaration of Independence proclaimed, "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness."

Out of necessity the Continental Army would seek manpower from the diverse populations of the colonies—to include enslaved and freed Blacks as well as Indigenous peoples. The Nation began with gathering Soldiers from different races, ethnic groups, and nationalities. They joined in the hope of being members of a free and just society.

This century began with a unifying call to arms following the attacks of September 11, 2001. The Army ranks were subsequently filled with volunteers from across the national landscape of race, ethnicity, and creed. We imagined a post-racial society with the election of the first African American President in 2008 and sought evidence in the photos of “Brothers at War” with the slate of Black general officers at the helm of theater operations in the war on terror. Three Black Army officers assumed the prestigious four-star rank, in charge of unified and subunified combatant commands and a major Army command.¹ However, although the Army may boast and showcase minority individuals as leaders within the force, diversity, equity, and inclusion achievements cannot be taken for granted.

Accordingly, the Service identified diversity as a strategic outcome in its *Army People Strategy*, noting that “the Army is committed to equality of opportunity, providing all of our talented people with fulfilling and rewarding professional careers. As an inclusive and representative American institution, we ensure that our people possess a diversity of *talent*—knowledge, skills, behaviors, and preferences—drawn from all corners of our country and its vibrant, diverse population.”²

The path for African American Soldiers—officer and enlisted—has been a long and arduous one. This article chronicles elements of that journey from its beginning with the American Revolutionary War through to the present day. It highlights the challenges, progress, and ever-present threats of regression encountered along the path of service. The aspirations of current diversity, equity, and inclusion (DEI) efforts will require awareness, intentionality, and

commitment to bring to fruition. While the Army boasts of its “tradition as a global leader in DEI,”³ the focus must be on “Deeds, Not Words.”⁴

The Army’s record on this issue, in both deeds and words, is mixed. In times of national crisis, the Army is among the first institutions to seek greater service and sacrifice from African Americans and in return to promise greater equality. But once the crisis passes, the Army has often been slow to serve as an engine of racial equality. This cycle nevertheless offers a kind of halting advance. Following each crisis, the retrenchment phase never fully returns the repression to the status quo ante; like waves on the beach during a rising tide, each makes incremental progress. Today’s Army leaders should become familiar with the role of the Service both in creating opportunity and—too often—in denying its full fruits to all Soldiers. Only by understanding this history can today’s Army leaders build a climate and a culture of true equality of opportunity.

Building on and updating the work of Charles C. Moskos and John Sibley Butler, this article surveys the Army’s mixed history as a provider of opportunity for racial integration and equal opportunity, beginning with General George Washington’s decision to forbid the recruitment of Black Soldiers into the Continental Army and following through to today’s disproportionately limited number of Black combat arms officers.⁵ Throughout American history, as David Halberstam notes in his foreword to Gail Buckley’s invaluable *American Patriots*, African Americans “remained loyal to concepts of freedom and democracy even when they were the most marginal beneficiaries of the very ideals they were defending.”⁶ Their experience should inspire today’s military leaders to build on their achievements and institutionalize the Army’s role as a leader in forming a more perfect union for all of America’s citizens.

The Birth of the Army and the Birth of America

Racism is America’s original sin.⁷ Long before independence, colonial legis-

latures passed laws governing every aspect of the slave trade. Colonial militias formed patrols to capture escaped slaves and suppress slave insurrection. In the face of such repression, the role of African Americans in the American Revolution is indeed remarkable. Crispus Attucks was the first American to die by British gunfire in the Revolution, cut down by Redcoat muskets at the Boston Massacre of 1770. As tensions continued to rise and the colonists decided to fight back, Prince Estabrook was wounded at the Battle of Lexington and Concord on April 19, 1775. Following “the shot heard round the world,” Massachusetts was desperate to create a force capable of resisting the British Empire. The colonial legislature opened the way to recruit free Black men to the state militia, and many of these recruits served at the Battle of Bunker Hill. On June 14, 1775, the Continental Congress authorized the raising of six companies of riflemen to join the Massachusetts militiamen around Boston, thereby creating the Army. Out of necessity, the colonial Army was created as a racially integrated institution in a racially segregated society. Black Americans volunteered to serve in this institution with their eyes open, fully aware of the injustices of their society yet hopeful that military service would create a more perfect union for themselves and their posterity.

African American Soldiers in the Revolution

Washington read two reports every day.⁸ One was the intelligence report derived from his carefully cultivated network of spies. The second was the strength report, showing the size and effectiveness of the Continental Army. When Washington took command, in June 1775, both reports gave cause for optimism. On the heels of Lexington and Concord, Massachusetts militiamen flocked to the hills overlooking Boston. The newly formed Continental Army would fight the British to a standstill at Bunker Hill and ultimately compel the British to evacuate Boston. Soon after

taking command, Washington bowed to political pressure and issued a decree forbidding the recruitment of Blacks into the Continental Army.

By January 1777, however, the reports Washington read were bleak. Injuries, illness, and diminishing patriotic zeal had thinned the ranks of the Continental Army. The British commanded the seas and occupied every major population center in the United States. At the outset of the war, the royal governor of Virginia issued a decree promising freedom to any African American held in slavery who would flee bondage and fight for the Royalist cause.⁹ Facing military defeat and constrained by necessity, Washington reversed his earlier decree and permitted Black Soldiers to serve.¹⁰ Ultimately, Black Americans would constitute 5,000 of the roughly 230,000 Soldiers to fight for independence, even though that independence would not extend to Americans of African descent.¹¹ The colonial Army was likely the most integrated the Army would be until the Korean War, according to Glenn Williams of the U.S. Army Center for Military History.¹² Nonetheless, in 1787, the U.S. Constitution codified slavery and forbade any legislation regulating the slave trade for another 20 years.

The Constitution and the Institutionalization of Repression

The first half of the 19th century witnessed the expansion and reinforcement of slavery throughout the United States. The Constitution institutionalized slavery with the infamous Three-Fifths Compromise and prohibited any restriction of the slave trade until 1808. For much of the first half of the 19th century, the Army remained a small constabulary force with little impact on national policy. The sole exception to this pattern was during the War of 1812, when, as in the Revolution, the United States turned to Black residents for support. Black Soldiers served in both integrated and all-Black regiments, while Black laborers served in construction and logistics roles. Once

the crisis had passed, Black Soldiers were largely mustered out of the Army.

The Haitian Revolution of 1791¹³ and Nat Turner's slave rebellion of 1831¹⁴ created enormous fear of slave rebellion, fueling the demand for slave patrols to prevent insurrection. State militias continued their practice of providing leaders and manpower for slave patrols, particularly in Virginia and South Carolina. Indeed, both the Citadel and the Virginia Military Institute were founded for the express purpose of providing a command structure for slave patrols.¹⁵ The passage of the Fugitive Slave Act in 1850 strengthened the legal standing of slave patrols for hunting escaped slaves and crushing any incipient slave rebellions.

African American Soldiers in the Civil War

As in previous conflicts, the U.S. Government initially minimized service opportunities for Black Soldiers in the Civil War.¹⁶ President Abraham Lincoln only grudgingly admitted Black Soldiers to manual labor and other service and support roles. This concession was hardly an act of enlightenment; the Confederacy employed enslaved men in the same roles.¹⁷ Union General George McClellan went so far as returning fugitive slaves to their Confederate masters.

The exigencies of war and the agency of individual Black men and women, however, forced the Union to reverse these policies. The Union's battlefield ineptitude and heavy losses forced the steady, bottom-up incremental expansion of the roles Black Soldiers played on the battlefield. Individual commanders, pressed for manpower, began using Black troops in combat roles. Some even issued decrees of emancipation far ahead of Lincoln's famous proclamation. This trend culminated in the formation of Black regiments, perhaps most notably the 54th Massachusetts. Led by White officers and paid less than their Union compatriots, these regiments nevertheless performed heroically in combat. Black leaders had long understood the importance of military service in achieving full citizenship. Frederick Douglass was

a leading advocate of the formation of Black regiments, and his son would serve as the command sergeant major of the 54th Massachusetts.¹⁸

Beyond the battlefield, individual Black men and women escaping slavery compelled a change in Union policy. As Union armies moved south, slaves escaped to seek their protection and serve in their ranks. Lincoln's Emancipation Proclamation merely codified in policy what was already evident on the battlefield: Black men and women were not the property of their purported masters but were individual human beings with autonomy and agency. They played an invaluable role in the ultimate outcome of the conflict, constituting about 10 percent of Union forces, with some 190,000 in the Army and 19,000 in the Navy. Nearly 40,000 perished in their fight for freedom.¹⁹ There is no support—none whatsoever—for the trope that *any* served willingly for the Confederacy.

Black Citizens and Soldiers During Reconstruction

The issue of Black enfranchisement was central to Reconstruction in the postwar South. In the last speech before his assassination, Lincoln advocated granting the franchise to those Black men who were "very intelligent, and on those who serve our cause as Soldiers."²⁰ With the ratification of the 13th, 14th, and 15th Amendments to the Constitution, Black men gained full citizenship in law. Some 2,000 Black men served in political office from 1867 to 1876, from the local level up to the Senate.²¹ Black citizens made substantial gains in education, health, and literacy, aided by the Freedmen's Bureau.

While Black citizens' economic, social, and political gains were never equal to their numbers or their contributions, the pace of progress in this brief era was nevertheless remarkable. The achievement of full citizenship varied greatly depending on local conditions, and no condition was more important than the presence of Black Soldiers. Simply put, where Black Soldiers served, Black citizens thrived. Black Soldiers safeguarded their fellow citizens from voter suppression, enabling



On USS *Stockholm*, nine Soldiers of 369th Infantry Regiment, awarded French government's Croix de Guerre for gallantry in action, pose for photo while awaiting disembarkation in New York City, February 12, 1919; left to right, front row, Private Ed Williams, Private Herbert Taylor, Private Leon E. Fraiter, Private Ralph Hawkins; back row, Sergeant Henry David Primas, Sr., Sergeant Daniel W. Storms, Jr., Private Joe Williams, Private Alfred S. Manley, and Corporal Tyler W. Taylor (U.S. National Archives and Records Administration)

the full exercise of the franchise. Black Soldiers guaranteed their fellow citizens' liberty and property, enabling educational and economic advancement. However, even this halting and limited progress proved too much for many Whites. Following a close and disputed election in 1876, Rutherford B. Hayes secured the White House through a "corrupt bargain." In exchange for the support of Southern Democrats, Hayes would effectively end Reconstruction in the South.

Jim Crow and the Black Codes

Even before the 1876 corrupt bargain, the halting progress Blacks achieved during Reconstruction was fomenting a White backlash. Often led by former Confederate officers, terrorist groups such as the Red Shirts and the Ku Klux Klan emerged to intimidate Black citizens attempting to exercise their rights in the South. With the end of Reconstruction and the withdrawal of the Union Army from the South, these

efforts accelerated with a vengeance. Every former Confederate state passed "Black codes," creating an apartheid system that regulated virtually every aspect of public life along racial terms—voting, jury duty, property sales, and every public accommodation from restaurants to toilets. Local law officials enforced these codes with the assistance of the same terrorist groups attacking Black citizens in the exercise of their rights.



Pilots of elite, all-Black 332nd Fighter Group, “Tuskegee Airmen,” at Ramitelli, Italy; left to right, Lieutenant Dempsey W. Morgan, Lieutenant Carroll S. Woods, Lieutenant Robert H. Nelson, Jr., Captain Andrew D. Turner, and Lieutenant Clarence P. Lester, August 1944 (U.S. Air Force)

Black Soldiers and veterans were targeted with vehemence in these terror campaigns. Vigilante groups would murder these men in grisly public spectacles with total impunity, with either tacit or overt support from local county sheriffs. These terror campaigns extended beyond the South and were particularly intense wherever large concentrations of Black Soldiers or veterans were found. Although forming “colored” regiments and admitting Black cadets to West Point, the Army turned a blind eye to the hazing and harassment that too many Black Soldiers suffered.²² Despite this sustained campaign of societal terror, Black Americans sowed the institutional seeds that would flower in times of later national crises, including Booker T. Washington’s Tuskegee Institute.

Buffalo Soldiers and the Rise of the African American Professional Soldier

Paradoxically, the terror campaign waged against Blacks in American society coincided with the emergence of the Black professional Soldier. An 1866 act of Congress established two regiments of Black infantry (the 24th and 25th) and two regiments of Black cavalry (the 9th and 10th). Previous eras had seen Black Soldiers enlisted in moments of crisis and mustered out the moment the crisis passed. These Soldiers, however, would be long-serving professionals. The cavalrymen would earn the moniker “Buffalo Soldiers” from their Native American adversaries, with the comparison to the sacred animal a mark of high respect.

Both the Black infantry and cavalry regiments served with distinction on the American frontier and in the Spanish-American War. Members of the regiments distinguished themselves when detailed to instructor duty. Black infantrymen were renowned for their marksmanship ability, and the cavalrymen served as riding instructors at West Point. Whether in the field or on instructional assignments, they often served alongside White Soldiers in close quarters. While far from achieving full integration and social equality, Black Soldiers nevertheless earned a degree of social status unthinkable not only in former Confederate states but also anywhere else in American society. This relative equality frequently rankled local White communities, resulting in conflicts

ranging from small disputes over public accommodations to crises such as the infamous Brownsville Affair in 1906, when Buffalo Soldiers were falsely accused of murder and assault.²³

Black Doughboys, More at Home “Over There” Than Here

As in previous conflicts, America’s racism and its manpower needs collided in World War I, and the latter eventually overwhelmed the former. President Woodrow Wilson was a virulent racist²⁴ who did not believe Black men possessed soldierly qualities. In the curious logic of racism acquired in his native Virginia, Wilson viewed Black men as both dangerous and cowardly. However, when the United States entered World War I, the manpower needs of the Allied Expeditionary Force demanded a massive conscription program without regard to race. Indeed, Black conscripts were more likely than their White counterparts to be found fit for service.²⁵ Whenever possible, Black Soldiers were consigned to service and support roles rather than assigned direct combat duties. Nevertheless, the Army fielded two Black infantry divisions, the 92nd and 93rd, both of which were led in part by Black officers. While the 92nd was embroiled in controversies not completely of its own making, the 93rd Infantry Division won broad acclaim. The division’s first regiment, the 369th, earned the nickname “Harlem Hellfighters.” At least 71 members of the regiment received the French Croix de Guerre. In August 1917, Wilson pressured General John Pershing to issue a directive to the French military warning against decorating Black Soldiers to too great an extent for fear of “spoiling the Negroes.” The French largely ignored this directive, valuing Black Soldiers not only for their battlefield heroism but also for a gift that would continue long after the war ended: American jazz.

The Invisible Empire Strikes Back

When Black Doughboys returned home, their service was not forgotten but instead was actively resented by

White America. Wasting no time, a White mob attacked returning Black Soldiers during a homecoming ceremony in Norfolk, Virginia, in the summer of 1919. The Doughboys’ return saw White mobs murder more than a dozen Black veterans. These incidents occurred in the context of the so-called Red Summer of 1919, with White mobs terrorizing Black communities on the smallest pretext or no pretext at all. The massacre in Elaine, Arkansas, alone accounted for as many as 100 deaths among African Americans. And throughout the 1920s, membership in the Ku Klux Klan and other White supremacist organizations exploded.

Beyond the campaign of violence and intimidation, White supremacists during this era waged a psychological campaign of “Lost Cause” mythology to glorify the Confederacy and White supremacy more generally. This campaign was waged on film, with D.W. Griffith’s *Birth of a Nation* released in 1915. It occurred in literature, with Margaret Mitchell’s *Gone with the Wind* published in 1936 (and subsequently made into a box office smash movie in 1939). This psychological campaign relied heavily on iconography, as the period from 1890 to 1920 saw large numbers of memorials to Confederate officers erected throughout the South. The Army played its part as well during this time, naming several military installations after Confederate generals: Camp Beauregard (1917), Fort Benning (1917), Fort Bragg (1918), Fort Gordon (1917), and Fort Lee (1917).²⁶

African American Soldiers in World War II

As war clouds gathered in the late 1930s, African American leaders saw a familiar pattern recurring. As Washington, Lincoln, Wilson, and others had done before, President Franklin D. Roosevelt would call upon Black Americans to serve and sacrifice in the name of freedom, with only the smallest sense of irony. Black leaders met these demands with a level of preparation and organization heretofore not achieved. They demanded greater integration of

the Armed Forces and greater inclusion in the burgeoning defense industry.

When the United States entered World War II, in 1941, African Americans were not content merely to fill the service and support roles to which they had long been relegated. Forced to choose between maintaining its racial caste system and winning the war, the Army reluctantly chose the latter. The 92nd Infantry Division, known as the Buffalo Soldier Division, was part of a segregated Army where Black Soldiers were assigned to formations under the command of White officers. Whereas several accounts disparage the performance of African American units in World War II, future general officer Frederic Davison commented, “We [the 366th Regiment] had two enemies to fight. We had to fight the Germans in the Apennines, and we had to fight the 92nd Division hierarchy.”²⁷ In his judgment, “it almost seemed as though there was a design for failure” as units of the division were ill trained and under poor senior leadership.²⁸

Other Black Army units, however, distinguished themselves and were grudgingly acknowledged for their significant performance in the European theater of war. The Tuskegee Airmen flew 1,600 combat missions over Europe, and the 761st Tank Battalion fought in General George Patton’s dash across France and daring counterattack during the Battle of the Bulge. Black Soldiers also continued their service in support roles; Patton’s success at the Bulge would not have been possible but for the mostly Black truck drivers hauling fuel in the convoy system called Red Ball Express. These heroics notwithstanding, the Army maintained as much racial segregation as it could, going so far as maintaining separate blood banks. The war produced at least two generations of Black leaders who would alter the shape not only of the Army but of American society as well. Benjamin O. Davis, Jr., commanded the Tuskegee Airmen during the war and became the first Black general in the newly formed Air Force following the war. He followed in the footsteps of

his father, Benjamin O. Davis, Sr., the Army's first Black brigadier general. In the waning days of the war, the Army court-martialed a Black lieutenant for refusing to sit in the colored section in the back of the bus. His name was Jack Roosevelt Robinson.

The Desegregation of the Armed Forces

Many Black World War II veterans were confronted with violence on the trains and buses that carried them home from the war. Civil rights organizations such as the National Association for the Advancement of Colored People took up the cause of defending Black veterans. Throughout the war, civil rights groups had adopted the "Double V" campaign, fighting for democracy abroad and equal rights at home.²⁹ With the former goal achieved, the latter came to the forefront.

In the wake of victory in Europe and Japan, civil rights groups pressured President Harry Truman to defend returning Black veterans against violence and discrimination. Truman was no natural ally of civil rights, having absorbed long and deeply held racist sentiment from his native Missouri. Nevertheless, due both to the injustice of the treatment Black veterans suffered at the hands of their own countrymen and to a desperate need for Black votes in the 1948 election, Truman formed a Presidential commission on civil rights in 1946. This commission recommended an end to racial segregation in the Armed Forces. On July 26, 1948, over the objections of "Dixiecrats" within his own party, Truman signed Executive Order 9981, officially ending racial segregation in the U.S. military. Truman's political calculus proved correct, if narrowly so: the Black vote was instrumental in his razor-thin victory over Wendell Willkie. But the Services slow-rolled the implementation of the order. Truman's Secretary of the Army Kenneth Royall stated, "The Army is not an instrument for social evolution."³⁰ The last segregated unit in the Armed Forces was the Army's 94th Engineer Battalion, which finally complied with Truman's order in 1954.

The Korean and Vietnam Wars

The U.S. Army in both Korea and Vietnam simultaneously reflected and challenged the racism so ubiquitous in American society. In defiance of Truman's executive order, the Army at the outset of the Korean War was largely segregated along racial lines. Army units were ill prepared at the outset of the Korean War, and most performed poorly. However, Army commanders singled out the all-Black 24th Infantry Regiment for special opprobrium, disbanding the unit and reassigning its Soldiers to majority-White units. Juxtaposed with such casual racism, the Army saw Black commanders leading White Soldiers in combat, including Distinguished Service Cross recipient First Lieutenant Ellison C. Wynn. Pressed by necessity, the Army began integrating combat units and assigning Soldiers without consideration to race.

The Army continued this practice in Vietnam, well ahead of an American society struggling to defend deeply held segregationist laws and customs. Nevertheless, during the Vietnam War, Blacks were more likely to be drafted, assigned to combat units, and court-martialed than were their White counterparts, and they were significantly underrepresented in the officer ranks. Black Soldiers and officers who fought with distinction included Captain Riley Leroy Pitts, the first Black officer to be awarded the Medal of Honor, and Lieutenant Colonel Charles Calvin Rogers, also awarded the Medal of Honor, who retired as a major general.³¹ As had been the case in Korea, integrated units performed well. Paradoxically but perhaps not surprisingly, racial tensions were more common in rear areas than among front-line combat forces. Perhaps no incident reflects this tension more clearly than the uprising in Long Binh Jail, where racial tensions exploded in 1968, leaving 1 dead and more than 100 injured.³²

The All-Volunteer Force and the Triumph of Market Forces

The Army emerged from Vietnam determined to purge itself of every aspect of the war's legacy, from doctrine

to manpower policy. No measure was more important in this process than the abandonment of conscription in favor of the All-Volunteer Force (AVF). Stung by the indiscipline and poor motivation of conscripts, the Army sought to recruit young people who saw the Service as offering a path to a better life. This appeal proved especially effective for African Americans, who were disproportionately represented in the enlisted ranks of the AVF. To its credit, the Army created a meritocracy less affected by racism than that of any other comparably sized institution in American society. Millions of African Americans served honorably and with distinction, with a few, most notably Colin Powell, wearing general's stars. Twenty years after the establishment of the AVF, sociologist Charles Moskos offered his observation that "only in America do Blacks routinely boss Whites" as evidence of the progress of affirmative action in the U.S. Army.³³

Nevertheless, the AVF proved at best a mixed success in racial relations. Powell and a few others notwithstanding, African Americans to this day remain underrepresented in the senior ranks of the Army. Decades after the abolition of formal racial barriers to combat duty, African Americans remain overrepresented in service and support roles and underrepresented in combat units. This trend is especially prevalent in elite special operations forces, which remain predominantly White. The AVF relied on market forces to fill its ranks, allowing recruits to fill the roles where they felt most welcome. Ironically, the admirable degree of autonomy in the AVF produces some of the very same outcomes as formal policies of racial segregation.

Operations Desert Storm, Iraqi Freedom, and Enduring Freedom

In 1991, the AVF went to war, and it has remained at war continuously ever since. The Army viewed the 1991 Gulf War as an affirmation of its purging the ghosts of Vietnam. In the Army's telling, a well-led, well-trained volunteer force destroyed the



Men of 24th Infantry Regiment move up to firing line in Korea, July 18, 1950 (U.S. Army Signal Corps/U.S. National Archives and Records Administration)



Private First Class Milton L. Cook, from Company C, 1st Battalion, 5th Mechanized Infantry, 25th Infantry Division, fires M60 machine gun while on search and destroy mission as part of Operation Cedar Falls, conducted in and around Filhol Plantation near Cu Chi, Republic of Vietnam, January 8, 1967 (U.S. National Archives and Records Administration)

Iraqi army in 100 hours of ground combat, affirming its post-Vietnam reforms. Similarly, the Army views the performance of the AVF in Iraq and Afghanistan as exceeding all expectations. The AVF was never designed for sustained combat over the course of decades; its designers assumed that such conflict would necessitate the return of conscription. While there is much to recommend this perspective, it is nevertheless incomplete. As was the case in the segregated Army, African Americans are less likely to serve as officers, more likely to serve in support roles, and far more likely to be court-martialed than their White counterparts.³⁴ African Americans take great pride in being overrepresented in

the ranks of the military, but even this point of pride comes with a caveat. Americans rightly worry that the Army is becoming isolated from the society that it serves.

Toward a More Perfect Union: The Army as an Anti-Racist Institution

The history of racial integration in the Army is mixed; it adopted policies of racial equality when it needed combat readiness the most, only to retreat at least in part from those commitments once the crisis passed. The Army can and should be both proud of the role it has played in creating equality of opportunity for Soldiers of all colors, races, and creeds and simultaneously con-

scious of the fact that it has not done all that it can in the pursuit of that goal.

The Army can do more to accomplish its avowed goal of “providing all of our talented people with fulfilling and rewarding professional careers.”³⁵ It can begin by acknowledging its role in the often racist policies and practices of the past. Positive next steps would include redefining recruitment policies with the explicit goals of achieving racial equality in the highest ranks and highest-profile missions of the Army, redesigning the Army’s organizational culture to purge the institution of Confederate base names that celebrate slave-holding traitors in military history, reexamining the heroes it celebrates, and recognizing the agency of individual Black citizens and Soldiers

acting from a burning desire for freedom and marked by a willingness to pay for that freedom with their blood.

America would likely not exist today as a free and united country were it not for the courage and service of Black Soldiers throughout its history. They deserve more recognition and more gratitude for the role they have played in helping form a more perfect union—a fight that continues today. JFQ

Notes

¹ Lloyd Austin, Commanding General, U.S. Central Command, and now Secretary of Defense; Dennis Via, Commanding General, Army Materiel Command; and Vincent K. Brooks, Commanding General, U.S. Forces Korea.

² *Army People Strategy* (Washington, DC: Headquarters Department of the Army, October 2019), 5–6, available at <https://issuu.com/usarmypeople/docs/army_people_strategy_2020_7fac48d631b9c0?fr=sZmU4YzIwNjE1Mg>.

³ *Army People Strategy: Diversity, Equity, and Inclusion Annex* (Washington, DC: Headquarters Department of the Army, September 1, 2020), 3, available at <https://www.army.mil/e2/downloads/rv7/the_army_people_strategy_diversity_equity_and_inclusion_annex_2020_09_01_signed_final.pdf>.

⁴ “Deeds, Not Words” is the motto of the 22nd Infantry Regiment—an Army unit that was integrated with Black Seminole scouts.

⁵ Charles C. Moskos and John Sibley Butler, *All That We Can Be: Black Leadership and Racial Integration the Army Way* (New York: Basic Books, 1996).

⁶ David Halberstam, “Foreword,” in Gail Buckley, *American Patriots: The Story of Blacks in the Military From the Revolution to Desert Storm* (New York: Random House, 2002), ix.

⁷ Nikole Hannah-Jones et al., eds., *The 1619 Project: A New Origin Story* (New York: One World, 2021).

⁸ See Benjamin Quarles, *The Negro in the American Revolution* (Chapel Hill: University of North Carolina Press, 1961).

⁹ See the November 7, 1775, Proclamation of John Murray, Earl of Dunmore, in “Africans in America,” PBS, available at <<https://www.pbs.org/wgbh/aia/part2/2h42t.html>>.

¹⁰ Elizabeth M. Collins, “Black Soldiers in the Revolutionary War,” *Army.mil*, March 4, 2013, available at <https://www.army.mil/article/97705/black_soldiers_in_the_revolutionary_war>.

¹¹ See “The Revolutionary War” in “Africans in America,” PBS, available at <<https://www.pbs.org/wgbh/aia/>

part2/2narr4.html>.

¹² Collins, “Black Soldiers in the Revolutionary War.”

¹³ “1784–1800: The Diplomacy of the Early Republic,” Office of the Historian, Department of State, available at <<https://history.state.gov/milestones/1784-1800/foreword>>.

¹⁴ Jennifer L. Larson, “A Rebellion to Remember: The Legacy of Nat Turner,” in *Documenting the American South: Primary Resources for the Study of Southern History, Literature, and Culture*, University of North Carolina Library, available at <<https://docsouth.unc.edu/highlights/turner.html>>.

¹⁵ Robert Behre, “The Citadel’s Early Story,” *Post and Courier*, March 25, 2018, updated September 14, 2020, available at <https://www.postandcourier.com/news/the-citadels-early-story/article_21ae8ca2-1bfb-11e8-b533-2f6d6042759a.html>.

¹⁶ Good sources include Benjamin Quarles, *The Negro in the Civil War* (Boston: Little, Brown, 1953), and George W. Williams, *A History of the Negro Troops in the War of the Rebellion, 1861–1865* (New York: Negro Universities Press, 1888).

¹⁷ Buckley, *American Patriots*, 81. This book, written by the daughter of civil rights activist Lena Horne, is an invaluable source on this topic. A shorter argument that parallels the one in this book can be found in Paul-Thomas Ferguson, “African American Service and Racial Integration in the U.S. Military,” *Army.mil*, February 23, 2021, available at <https://www.army.mil/article/243604/african_american_service_and_racial_integration_in_the_u_s_military>.

¹⁸ “Lewis Henry Douglass,” Library of Congress, available at <<https://loc.gov/exhibits/civil-war-in-america/biographies/lewis-henry-douglass.html>>.

¹⁹ “Black Soldiers in the U.S. Military During the Civil War,” National Archives and Records Administration, September 1, 2017, available at <<https://www.archives.gov/education/lessons/blacks-civil-war>>.

²⁰ Sarah Pruitt, “What Lincoln Said in His Final Speech,” *History*, April 10, 2015, available at <<https://www.history.com/news/what-lincoln-said-in-his-final-speech>>.

²¹ Eric Foner, *Reconstruction: America’s Unfinished Revolution, 1863–1877* (New York: Harper Perennial, 2014).

²² For the tragic but inspiring story of the first Black graduate of West Point, see Charles Allen, “The Legacy of Henry O. Flipper in the U.S. Army,” *Army.mil*, June 14, 2010, available at <https://www.army.mil/article/40763/the_legacy_of_henry_o_flipper_in_the_u_s_army>.

²³ Richard Wormser, “The Brownsville Affair,” Thirteen Media With Impact, available at <https://www.thirteen.org/wnet/jimcrow/stories_events_browns.html>.

²⁴ Dick Lehr, “The Racist Legacy of

Woodrow Wilson,” *The Atlantic*, November 27, 2015, available at <<https://www.theatlantic.com/politics/archive/2015/11/wilson-legacy-racism/417549/>>.

²⁵ Jami L. Bryan, “Fighting for Respect: African-American Soldiers in World War I,” National Museum of the United States Army, available at <<https://armyhistory.org/fighting-for-respect-african-american-soldiers-in-wwi/>>.

²⁶ Mike Jason, John Nagl, and Paul Yingling, “Dear Mr. Secretary, You Can Rename Army Bases Right Now,” *Defense One*, June 9, 2020, available at <<https://www.defenseone.com/ideas/2020/06/dear-mr-secretary-you-can-rename-army-bases-right-now/166025/>>.

²⁷ Charles D. Allen, “Army 2-Star Made History Before, After Military Integration,” *Military Times*, January 31, 2018, available at <<https://www.militarytimes.com/military-honor/black-military-history/2018/01/31/army-2-star-made-history-before-after-military-integration/>>.

²⁸ *Ibid.*

²⁹ “The Double V Victory,” The National WWII Museum, available at <<https://www.nationalww2museum.org/war/articles/double-v-victory>>.

³⁰ Farrell Evans, “Why Harry Truman Ended Segregation in the U.S. Military in 1948,” *History*, November 5, 2020, available at <<https://www.history.com/news/harry-truman-executive-order-9981-desegregation-military-1948>>.

³¹ Charles D. Allen, “Maj. Gen. Charles C. Rogers: Talent Through Diversity, Equity, and Inclusion,” *Military Times*, January 28, 2021, available at <<https://www.militarytimes.com/opinion/commentary/2021/01/28/maj-gen-charles-c-rogers-talent-through-diversity-equity-and-inclusion/>>.

³² Sarah Kramer, “The Forgotten History of a Prison Uprising in Vietnam,” NPR, August 29, 2018, available at <<https://www.npr.org/sections/codeswitch/2018/08/29/642617106/the-forgotten-history-of-a-prison-uprising-in-vietnam>>.

³³ David Martin and Dan Rather, “Eye on America (Affirmative Action/United States Army),” *CBS Evening News*, May 31, 1995.

³⁴ Helene Cooper, “African Americans Are Highly Visible in the Military, but Almost Invisible at the Top,” *New York Times*, May 25, 2020, available at <<https://www.nytimes.com/2020/05/25/us/politics/military-minorities-leadership.html>>.

³⁵ *Army People Strategy*, 5–6.



Marines push through simulated riot during nonlethal weapons training course at Camp Lejeune, North Carolina, November 18, 2016 (U.S. Marine Corps/Victoria Ross)

Intermediate Force Capabilities Nonlethal Weapons and Related Military Capabilities

By Sara McGrath

The U.S. military has a history of fighting wars and winning battles through the overwhelming use of force. In today's strategic environ-

ment, however, the battle is often one of competition below the threshold of armed conflict. Our adversaries are gaining the advantage by exploiting the predictable joint force responses, either showing force through military presence or employing lethal force. Both of these extremes are often ineffective against adversary competition.

Yet neither doctrine nor training prepares the joint force to employ force between these extremes. To protect current and future national political and military interests, the U.S. military must modify its mindset and tactics to gain the necessary tools for strategic competition, or the Nation risks losing its competitive advantage.

Colonel Sara McGrath, USMC, is an Analyst in the Joint Intermediate Force Capabilities Office, Quantico, Virginia.

In the current strategic environment, the application of lethal force is often not suitable against threats below the threshold of armed conflict. A more suitable option, intermediate force capabilities (IFCs), offers a proportional response through nonlethal and nondestructive means. Nonlethal weapons (NLWs) are a primary contributor to the application of intermediate force, but additional existing capabilities also support the concept. These capabilities—including information operations (IOs), electromagnetic warfare (EW), and cyber operations (COs)—together with NLWs, contribute to achieving political goals without the use of lethal force.¹ These capabilities are essential to joint operations in today's security environment, yet commanders hesitate to employ them. This hesitancy is due to a poor understanding of their applicability for threats below armed conflict and, furthermore, because of minimal doctrinal integration and a lack of training on their potential benefits. One way to enable the joint force to gain a better conceptual understanding of how to employ IOs, EW, COs, and NLWs is to integrate them *doctrinally* as IFCs and to promote them as suitable alternative solutions to lethal force in current and future strategic environments. To explore the applicability of intermediate force and its contributing capabilities to the security environment, the following analysis shows the potential contributions of NLWs, IOs, EW, and COs to the IFC concept and offers suggestions to improve their integration in joint operations.

Traditionally, the United States has viewed national security through distinct categories of peace or war. In the traditional construct, showing military presence is an acceptable method to preserve peace through deterrence without the use of physical force. Conversely, once adversaries cross the threshold of armed conflict, the military responds to the threat with lethal force, both appropriate and proportional in a wartime scenario. But against the current challenge of “long-term strategic competition” and adversary aggression below the threshold of armed conflict,

the line between war and peace blurs.² In this gray zone, the proper determination on the use of force is rarely easily made in the face of an adversary's coercion or aggression.³ Lethal force is often too aggressive in the gray zone, leaving the joint force without a suitable, proportional response to adversary competition and aggression. As a result, our adversaries can easily gain a strategic advantage by acting below the threshold at which the joint force would normally respond to traditional warfare.⁴ As an option to compete against the adversary, IFCs provide a flexible response that negates the adversary's advantage of operating below the threshold of armed conflict.

IFCs are suitable for use across the entire competition continuum. By employing capabilities between “presence and lethal force to enable combat arms and support warfighters with expanded and enhanced options to deter, suppress, and/or respond to adversary action,”⁵ IFCs offer alternatives below the threshold of armed conflict: a nonlethal response option to adversaries' coercive tactics, misinformation, and sabotage.⁶ They also enable U.S. forces to ameliorate allied concerns and collaborate with affected partner nations against strategic competition. However, for IFCs to be effective, the joint force must shift its mindset from the sole employment of lethal force to “the mindset and capabilities necessary to succeed” in the competition continuum.⁷ This perspective shift will support adopting and employing an array of IFCs and doctrinally integrating the IFC concept into joint operations.

Conditions Achieved by IFCs

To compare the capabilities of NLWs, IOs, EW, and COs and to show their contributions to IFCs, there must first be an understanding of what intermediate force provides to the warfighter. In traditional warfare, using or threatening lethal force is a way to achieve strategic outcomes. In contrast, during gray zone operations, adversaries intentionally avoid lethal force, so as to achieve long-term strategic objectives. The intent of these unconventional methods of coercion is to exhaust opponents, breaking

political power or will, without a direct military confrontation.⁸ The joint force must counter strategic competitors' actions by managing escalation and fostering peaceful competition while also deterring the threat.⁹ Current doctrine and training do not sufficiently prepare the joint force to employ methods to counter this sort of competition without force escalation. With a better understanding of their employment, IFCs allow the joint force to achieve deterrence and de-escalation without unnecessary lethal force.

IFCs give warfighters the option to exert influence flexibly, when necessary, and to escalate or de-escalate as appropriate.¹⁰ IFCs' effects may include reducing collateral damage; deterring, defeating, or denying enemy access; and increasing decisionmaking space for the discriminate use of force.¹¹ IFCs provide a toolbox of both nonlethal and nondestructive means to achieve political objectives for competition below the threshold of armed conflict. Additionally, IFCs improve force protection, help maintain legitimacy and credibility, and assert friendly force influence. Still, for their effective employment, the joint force must have the knowledge and means to use all the options of IFCs.

Evaluating Components of IFCs

IFCs include an array of military capabilities. Exploring the component activities of NLWs, IOs, EW, and COs enables a comparison of each of these activities to the intended effects of IFCs. A summary of these effects includes four primary advantages: *reducing* unnecessary damage to personnel and/or infrastructure, *increasing* the time and distance for effective decisionmaking for maneuver or engagement, *deterring* or defeating adversary behavior, and *preserving* credibility and legitimacy for the United States and its partners and allies. NLWs provide all these advantages, but the method of employing IOs, EWs, and cyber and the type of effects they generate determine their ability to support intermediate-force capabilities. Although critical during armed conflict, destructive employment

or effects are often not appropriate for intermediate-force application scenarios. For example, physically destroying adversary command and control systems is a method of IOs, antiradiation missiles are a method of EW, and cyber activities can “rise to the level of use of force, with physical damage or destruction.”¹² These methods of employment create effects that go beyond the IFC level to lethal force. However, broadcasting messages is a form of IOs that is essential to IFCs; it allows friendly forces to influence the narrative and maintain the initiative in an otherwise ambiguous situation. Similarly, employing EW to deny an adversary’s ability to access command and control through the electromagnetic spectrum is critical to the success of the friendly mission. Finally, employing COs to protect and maintain control of network capabilities reduces unnecessary casualties by enabling situational awareness of friendly forces. The figure shows the

interrelationship of NLWs, IOs, EW, and COs as IFCs.¹³ Each of these capabilities contributes to a set of activities that support optimal IFC employment.

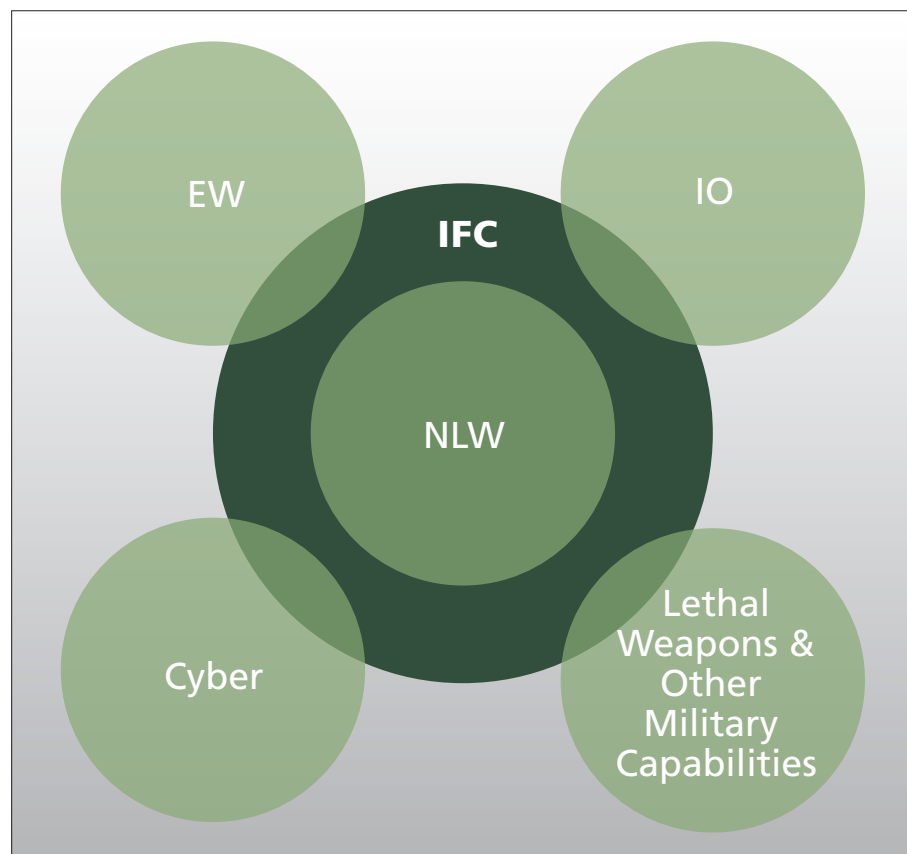
Nonlethal Weapons

NLWs are weapons, devices, or munitions explicitly designed and primarily employed to incapacitate personnel or materiel immediately while minimizing fatalities, permanent injury to personnel, and unnecessary damage to property.¹⁴ Despite the known operational benefits of NLWs, their employment has predominantly been by military police or law enforcement. Understanding additional employment options of NLWs against an asymmetric threat allows the joint force to recognize their full value. Specific applications include using long-range nonlethal directed-energy weapons to deter malign activity of adversaries that are using proxies to harass U.S. land or maritime forces. Other examples

include various crowd control devices, including multiple projectile munitions and grenades, laser ocular interrupters, auditory hailing devices, and vehicle-stopping devices.¹⁵ Additional improvements in technology—providing increased range, precision, and reliability—show promise for developments outside of these commonly known applications.¹⁶ Joint doctrine classifies NLWs as “additional capabilities” for nonlethal effects and recommends their integration to minimize both loss of life and property damage that could negatively influence public perception.¹⁷ This description of and recommendation for NLWs downplay and underemphasize the strategic role they have for maintaining favorable public perception and avoiding force escalation. The North Atlantic Treaty Organization (NATO) recognizes NLWs as a critical additional capability for meeting the demands of future operations and is currently advancing efforts for integrating IFCs into Alliance doctrine and planning.¹⁸ The joint force should follow NATO’s example and make a concerted effort to integrate NLWs and the IFC concept for successful operations below the threshold of armed conflict.

As a component of the IFC concept, NLWs offer a suitable approach when lethal force is unwarranted or undesirable, enhancing the commander’s ability to deter, deny, stop, disable, or de-escalate.¹⁹ Against a gray zone threat, NLWs *reduce* unnecessary damage through the discriminate use of force. Additionally, they *increase* decision space by offering an initial nonescalatory response for aiding in the determination of intent. Moreover, NLWs *deter* adversary behavior by providing a warning that adversary aggression is not acceptable. Finally, they *preserve* credibility and legitimacy by ensuring a level of force proportional to the situation. It is essential to understand that nonlethal fires do not eliminate the ability, nor the need, to use lethal force but instead provide strategic risk mitigation by creating the conditions to determine the necessary level of force.²⁰ In an organization

Figure. Intermediate Force Capabilities Interrelationships





Chief Electronics Technician Travis Hill operates console of Laser Weapon System aboard Afloat Forward Staging Base (Interim) USS *Ponce* to track Scan Eagle unmanned aerial vehicle, Arabian Gulf, July 13, 2017 (U.S. Navy/Joshua Bryce Bruns)

trained for the exceptional employment of lethal force, commanders must also recognize the value of NLWs as IFCs for a proportional military response below the level of armed conflict.

Information Operations

In traditional warfare, IOs are fundamental for facilitating physical maneuver during armed conflict. IOs also enable maneuver at all stages of crisis and below the level of armed conflict to increase the commander's options.²¹ Defined as the integrated employment of information-related capabilities to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries, IOs are essential to all military operations.²² NATO expands on this definition with the recognition that successful management of information influences all other elements of national power and is

essential to "maintaining Allied freedom of action."²³ Common methods of managing information within the operational environment include military information support operations, military deception, operational security, public affairs, and civil-military operations, among others.²⁴ Including an IO component of IFCs into an operational plan enables successful maneuver in both the physical and information spaces against the adversary threat.

IOs are a critical component of IFCs for friendly forces to advantageously influence and respond to ambiguous or threatening messaging. Enemy propaganda or coercion may prohibit friendly freedom of action in gray zone operations if not countered by friendly information. For example, an adversary may try to limit friendly use of novel technologies, such as directed energy, by

using fear tactics to turn public opinion against the employment of this NLW. Additionally, the proliferation of technology makes it easier for an adversary to access and manipulate information against friendly forces.²⁵ Strategic messaging by friendly forces attempts to counter these tactics. Just as NLWs can have a positive influence on public perception through limiting collateral damage, IOs can also have a positive influence if employed effectively.²⁶ Just as gaining the initiative in the physical domain is essential, it is essential that friendly forces control the effects of information to gain and maintain the initiative in the information environment—and thus maintain favorable public perception. Today, commanders must be able to optimize the positive effects of IO during strategic competition to gain the advantage for friendly forces.



Lieutenant Joanna Cruz, right, gives laser dazzler gun training to Quartermaster 1st Class Kahzia Johnson-Baker, aboard USS *Bunker Hill*, Pacific Ocean, January 24, 2020 (U.S. Navy/Nicholas V. Huynh)

IOs are an essential capability against competition below the threshold of armed conflict because of the conditions they achieve using intermediate force levels. Due to the “numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization,” the information environment is significant for shaping conditions in the gray zone.²⁷ IOs provide an immediate warning for *detering* adversary behavior. Additionally, IOs establish the conditions for friendly forces to gain global credibility or to publicly disapprove of adversaries’ illegal or coercive behavior, therefore *maintaining* their own legitimacy. Other examples of IO components of IFCs include preemptive strategic messaging to *reduce* collateral damage by facilitating maneuver away from a targeted area. In addition, employing messaging through novel technologies such as long-range auditory warning devices can *increase* a

commander’s decisionmaking space and time to determine adversary intent.²⁸ Just as the joint force employs IOs to support combat operations, it must adapt to a mindset of employing IOs as a component of intermediate force to control the information environment for friendly forces operating in the gray zone.

Electromagnetic Warfare

EW is an additional capability that contributes to IFCs by ensuring friendly use of the electromagnetic spectrum (EMS) in a confrontation below the level of armed conflict. During any engagement today, including those that fall below the threshold of armed conflict, friendly forces must have control of the EMS for effective operations.²⁹ Joint EMS operations facilitate the mission areas of EW and other activities that rely on the EMS, including certain activities that overlap between IO, cyber, and NLWs.³⁰ EW includes any activity in the EMS using radio waves, microwaves, millimeter waves, infrared radiation, visible light, ultraviolet radiation,

X-rays, and gamma rays.³¹ Divided into the subcomponents of electromagnetic attack, electromagnetic support, and electromagnetic protection, EW is defined in doctrine as military actions involving the use of electromagnetic and directed energy to control the EMS or to attack the enemy.³² In a similar definition, NATO also emphasizes that EW operations enhance situational awareness and protect friendly forces.³³ During gray zone operations, just as during traditional warfare, commanders may take for granted their ability to maneuver in the EMS. In the competition continuum, where control of the EMS is essential, intermediate force must include EW to facilitate physical maneuver and increase time and decision space for friendly forces.

Maneuver within the EMS is a critical capability for activities below the level of armed conflict. However, EW employment is often suboptimal in joint operations because of fear and a misunderstanding of its effects. Compounding the fear and misunderstanding,

innovation and investment in EW capabilities have waned during years of counterinsurgency.³⁴ Together, the minimal investment in modernizing EW and the fear of EW effects have caused their underuse within the joint force, with many commanders lacking knowledge and proficiency in EMS operations. Many simply assume that they will have full use of the EMS when needed. This situation must change so the joint force can become proficient at employing EW IFCs when appropriate. The joint force must understand the essential relationship of EW IFCs to the maneuver of friendly forces and recognize the critical role of the EMS against adversaries so that leaders have the knowledge and proficiency needed to operate in the EMS.

Employing EW as a component of IFCs creates opportunities across the competition continuum. EW that denies, degrades, or delays adversary systems provides viable intermediate force. However, EW tactics that include kinetic fires for the destruction of enemy systems, while potentially effective, are not appropriate for the level of force below armed conflict. More appropriate EW tactics, such as jamming adversary systems, *reduce* unnecessary casualties by denying enemy observation or targeting systems. EW employed for disruption against adversary weapons systems *deters* enemy capabilities used to harass, intrude, or assess friendly forces. Degradation of adversary communications or warning systems contributes to *increasing* the decisionmaking space for friendly force maneuver. Additionally, EW *preserves* EMS access to the information space for friendly use or denies access to the adversary. Finally, EW creates intermediate force through nonkinetic, nonlethal fires with reversible and nondestructive effects.³⁵ Each of these applications illustrates the critical interdependence of EW components of IFCs as an option against adversary gray zone activities. The joint force must capitalize on these capabilities to operate effectively against the adversary in the EMS in the strategic environment.

Cyber Operations

COs, the final capability considered here, make several contributions to

intermediate force with specific applications to the gray zone. Most COs create fires with little or no associated destruction through the interdependent network of information technology infrastructures and data.³⁶ Additionally, cyber targets include numerous critical aspects of the operational environment, such as the Internet, telecommunications networks, and computer systems.³⁷ In the operational environment, commanders conduct COs to retain freedom of maneuver in cyberspace, accomplish the JFC's objectives, deny freedom of action to enemies and adversaries, and enable other operational activities.³⁸ Similarly, NATO doctrinally recognizes COs for their essential contributions to "collective defence."³⁹ Each of these advantages of COs can contribute to IFCs, yet to use them effectively commanders must understand the types of cyber employment and the effects that best fulfill the intent of intermediate force.

Compared with traditional kinetic operations, COs have limited historical use in conflict. Given the scant operational case studies in this relatively new domain, their cyber effects and secondary effects are not entirely clear.⁴⁰ Although destruction of enemy networks is a potentially effective use of COs, this goal is not applicable to the concept of intermediate force. Additionally, studies suggest that certain applications of cyber may cause unintentional force escalation; these methods, too, do not meet the intent of intermediate force.⁴¹ The methods of COs best suited for IFCs include defensive operations to preserve friendly networks and offensive ones to degrade or deny adversary networks with nondestructive effects that reduce network capabilities. Cyber capabilities known for nondestructive effects will enable the joint force to gather information or employ targeted actions without lethality and are applicable across the competition continuum.⁴² In a situation where the strategic and operational goals are to minimize the use of lethal force and the resulting destruction, COs employed at intermediate force levels are most desirable. Employing COs' nondestructive

fires as a component of IFCs enhances joint operations against adversary competition—but only if commanders recognize their suitability and feasibility in the gray zone.

COs support the combined employment of multiple IFCs and contribute to achieving strategic objectives during gray zone operations. In such situations, cyber fires are similar to NLWs in *reducing* collateral damage and *detering* the adversary without lethal or destructive force.⁴³ Offensively conditioning the operational environment with COs enhances the effectiveness of other IFCs. Defensively, employing COs to protect friendly networks creates space for friendly forces to maneuver, *increasing* time and space for friendly operations in the physical domain. Educating and enabling the joint force to employ cyber fires in the gray zone is essential for countering strategic competition without escalating the level of force.

Scenario Analysis

The following is a theoretical example of IFCs' use in an operational environment. This scenario describes current capabilities of the joint force in a plausible operating environment to highlight the *integrated employment* of NLWs, IOs, EW, and COs. A commander must be knowledgeable about the options available within the IFC concept to achieve optimal conditions and delay force escalation.

U.S. and partner-nation naval forces are conducting freedom of navigation (FON) operations in an operational area bordered by multiple states with competing maritime claims. During these operations, friendly forces encounter a mixed contingent of adversary vessels including civilian, maritime militia, and fast-attack craft. The adversaries attempt to interfere with friendly flight operations and disrupt communications systems. The strategic objectives are to de-escalate tensions while conducting deterrence. The specified and implied tasks are to reduce harassing maritime activities, maintain credibility and legitimacy in the operational area, and enable partner

and allied nations to defend themselves without escalating to lethal force while preserving FON.

During operations, multiple unmanned aerial systems (UASs) approach a U.S. warship and interfere with friendly operations. To counter the UASs, friendly forces employ IFCs against them that include electronic attack to deny their observation capabilities, resulting in their departing the area. Using IOs as the second component of IFCs, friendly forces video and transmit the UAS swarm, broadcasting the harassing behavior to national news sources to influence public opinion against adversary tactics.

Despite the failed UAS intrusion, the fast-attack craft approaches U.S. ships at a high rate of speed. IFCs provide warning through NLWs by means of directed-energy vessel stopping and acoustic warning devices, delaying the approach of the vessels long enough for the friendly forces to determine adversary intent.⁴⁴ Additionally, the use of ongoing cyber-component IFCs during these operations protects friendly command and control networks against adversary cyber intrusion, allowing freedom of maneuver in cyberspace for the friendly and allied nations.

The decision to use IFCs in this scenario is in line with the strategic goal—in this case, to de-escalate the threat. The use of IFCs enables multiple proportional and suitable response options. IFCs preserve the credibility and legitimacy of friendly forces and reduce potential collateral damage. Furthermore, they open the decision space and allow time for commanders to determine if lethal force is suitable for the situation. If it is needed, there is nothing to prevent or prohibit the use of lethal force; however, using lethal force before it is warranted can damage the credibility of friendly forces. IFCs give the commander additional options to respond to a threat and de-escalate it.

An alternative playing-out of this scenario without the use of IFCs shows several points at which friendly force actions might result in force escalation. The

first is at the onset of the UAS intrusion. The second is at the approach of the fast-attack craft. It is possible that friendly forces could respond by firing warning shots toward the approaching adversary. These shots could be misinterpreted and met with force in response. The escalation continues until one side or the other crosses the threshold of lethal force. Ultimately, it is likely that the global perception of this incident would focus on the fact that friendly forces fired first. Unfortunately, firing a warning shot is a common response by a force not conditioned to think of alternate capabilities and by our partner nations faced with similar scenarios.

In the first example, by integrating the components of IFCs, including concurrent cyber protection to ensure situational awareness, EW to deter the UAS swarm, and NLWs to de-escalate the threat of the fast-attack craft, the joint force achieves the specified and implied tasks. Additionally, IOs in support of the strategic objectives help preserve credibility of friendly forces and maintain FON in the operating area. But because current doctrine leads the joint force to overlook the integration of NLWs, IOs, EW, and COs against an asymmetric threat, the alternate outcome of force levels escalating to lethal levels is a real possibility. To avoid escalating force levels, IFCs must be accessible across the joint force by commanders who understand each of the component capabilities and the applicability of IFCs when lethal force is not desirable.

Risks and Challenges

The above scenario illustrates the benefits of integrating IFCs into joint operations. However, as with any capability, there are associated risks. These include force management risk and future challenges risk.⁴⁵ The first risk stems from a hesitation to invest in nonlethal technologies and take on the associated challenge of training the joint force in those technologies. Conversely, if the United States does not equip its forces with new technologies and train them in those technologies' use, there is a risk that adversaries will quickly outpace the

United States in equipment, capabilities, and tactics. The second risk is due to the fundamental military perception on the use of lethal force. The perceived characteristic of any military force is that it is a lethal organization with no business in nonlethal capabilities.⁴⁶ One way to change this narrow mindset is to consider the perspective that war is a continuation of politics by other means.⁴⁷ The military must support political objectives in the gray zone, and, to do so effectively, the joint force must have suitable options below lethal force.

This same traditional military perception contributes to the idea that investment in nonlethal technologies takes away from investment in lethal ones. This perceived tradeoff comes with the risk that when a threat arises, the commander must choose between escalating the level of force or simply not responding to the threat. Neither of these options is ideal against an adversary that is skilled at warfare below the level of armed conflict. Lethal capabilities alone are not sufficient to equip the joint force for success. The fundamental perceptions that the military is equipped only for peace or war must change, so that the joint force can respond proficiently to adversary aggression with multiple capabilities, including IFCs, across the competition continuum.

Opportunities

The challenge of implementing IFCs also provides opportunities for the joint force. The Department of Defense has an opportunity to change how it views the poles of war and peace. Our adversaries excel in operations between the extremes. If the U.S. military cannot also operate between extremes, it will lose its competitive edge. We must become proficient in operating outside of these well-known and ingrained black-and-white confines, and doing so requires adopting new capabilities suited for the gray zone. Our current operating environment presents the joint force with the opportunity to expand available response options by investing in new technologies. Adopting new concepts and technologies will

support the evolution of the institutional mindset and improve operations against current and emerging threats. The evolving mindset will support the simultaneous changes needed in education and training for all leaders on IFCs and the concepts and technologies that support them in the strategic environment.⁴⁸ Realizing these opportunities will allow the United States to gain and maintain the advantage.

Doctrinal Integration

Capitalizing on the opportunity to integrate IFCs into the joint force requires assimilating the concept through doctrine, organization, training, materiel, leadership and education, personnel, and facilities. This process has begun with the

renaming, in March 2020, of the Joint Non-Lethal Weapons Directorate to the Joint Intermediate Force Capabilities Office to emphasize the importance of intermediate force to the current threat environment.⁴⁹ Additionally, in the tri-Service doctrine *Advantage at Sea*, published in 2020, Service leadership recognizes and recommends IFCs as an applicable concept.⁵⁰ Materiel investment continues for new IFC technologies that will provide additional means of influence. However, the momentum of these changes must continue; IFCs must be represented doctrinally more consistently as valid and plausible targeting options for commanders.

One recommendation for doctrinal integration is to introduce the concept of

“Intermediate Force” as the first heading under “Joint Fire Support and Force Capabilities” in Joint Publication 3-09, *Joint Fire Support*. Doctrinally identifying NLWs, IOs, EW, and COs emphasizes their contribution to intermediate force. The current doctrinal references are insufficient to highlight their contributions to combat operations and understate their importance for operations below the threshold of armed conflict. To improve the integration of NLWs, IOs, EW, and COs, doctrine should emphasize their contribution to IFCs. An explanatory paragraph describing intermediate force should define IFCs as “all domain,” suitable across the competition continuum and for employment by multiple platforms across the force. Emphasis should



Marine Corps Corporal Skyler Santori, amphibious assault vehicle mechanic assigned to Task Force Ellis, 1 Marine Expeditionary Force, fires Mossberg 500 pump-action shotgun during M104 nonlethal grenade live fire deck shoot aboard amphibious dock landing ship USS *Comstock*, Pacific Ocean, September 24, 2020 (U.S. Marine Corps/Manuel A. Serrano)



Army Reserve Master Sergeant Grant Smith, brigade operations sergeant for 290th Military Police Brigade, fires nonlethal rounds from M26-Modular Accessory Shotgun System during nonlethal weapons training, July 26, 2022, at Camp Shelby Joint Forces Training Center, in Mississippi (Arizona Army National Guard/Brian A. Barbour)



include the relevance of each of the capabilities against a gray zone threat, with an additional reference to the individual joint publication governing their standard employment. In offering intermediate force as an option *in addition to* lethal force but not *in place of* lethal force, the IFC concept becomes a suitable, applicable, trained response for future leaders.

Adversaries' actions across the competition continuum require the joint force to compete through options other than lethal force. Yet strongly held perceptions on the distinction between peace and war have left the U.S. military neither positioned nor prepared for competition below the level of armed conflict. To remain relevant, leaders must "evolve our approach to warfighting," meaning that we must broaden our perspectives and adopt new technologies and concepts that support such evolution.⁵¹ IFCs offer essential options to the joint force to deter and de-escalate adversary behavior when lethal force is not suitable. The U.S. military cannot continue to overlook these critical capabilities as tools of influence against the adversary, when the strategic goals are to de-escalate tension and avoid increasing the level of force. Without the option of intermediate force, U.S. national security goals are at risk. To mitigate this risk, the military establishment must continue to proliferate information and enhance the ability of the joint force to understand how intermediate force can gain the advantage for friendly forces in the strategic environment. JFQ

Notes

¹ John L. Barry, Michael W. Everett, and Allen G. Peck, *Nonlethal Military Means: New Leverage for a New Era* (Cambridge, MA: John F. Kennedy School of Government, 1994), 2, available at <[https://iif.harvard.edu/manifests/view/drs:469582318\\$4i](https://iif.harvard.edu/manifests/view/drs:469582318$4i)>.

² *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense [DOD], January 2018), 2, available at <<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>>.

- ³ Frank G. Hoffman, *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War* (Washington, DC: The Heritage Foundation, October 15, 2016), 26, available at <<https://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protracted-gray>>.
- ⁴ *Summary of the Irregular Warfare Annex to the National Defense Strategy* (Washington, DC: DOD, 2020), 2, available at <<https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF>>.
- ⁵ *Advantage at Sea: Prevailing With Integrated All-Domain Naval Power* (Washington, DC: Headquarters Department of the Navy, December 2020), 25, available at <<https://media.defense.gov/2020/dec/16/2002553074/-1/-1/0/triservicestrategy.pdf>>.
- ⁶ *Intermediate Force Capabilities: Bridging the Gap Between Presence and Lethality, Executive Agent's Planning Guidance 2020* (Quantico, VA: Department of Defense Non-Lethal Weapons Program, March 2020), available at <<https://mca-marines.org/wp-content/uploads/DoD-NLW-EA-Planning-Guidance-March-2020.pdf>>.
- ⁷ *Summary of the Irregular Warfare Annex to the National Defense Strategy*, 1.
- ⁸ *Ibid.*, 4.
- ⁹ Joint Doctrine Note 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), 5, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.
- ¹⁰ Wendell B. Leimbach, Jr., and Susan D. LeVine, "Winning the Gray Zone: The Importance of Intermediate Force Capabilities in Implementing the National Defense Strategy," *Comparative Strategy* 40, no. 3 (2021), 223–234.
- ¹¹ "Analytical Support to the Development and Experimentation of NLW Concepts of Operation and Employment," STO-TR-SAS-94, North Atlantic Treaty Organization (NATO) Science and Technology Organization, May 4, 2017.
- ¹² Allied Joint Publication (AJP)-3.10, *Allied Joint Doctrine for Information Operations* (Brussels: NATO, November 2009), I-10, available at <<https://info.publicintelligence.net/NATO-IO.pdf>>; Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), II-4, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf>.
- ¹³ Joint Professional Education Intermediate Force Capabilities Courseware Brief, Joint Intermediate Force Capabilities Office, Quantico, VA.
- ¹⁴ JP 3-09, *Joint Fire Support* (Washington, DC: The Joint Staff, April 10, 2019), GL-8, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf>.
- ¹⁵ *Multi-Service Tactics, Techniques, and Procedures for the Employment of Nonlethal Weapons* (Hampton, VA: Air Land Sea Application Center, May 2020), 7–11.
- ¹⁶ Leimbach and LeVine, "Winning the Gray Zone," 3–4.
- ¹⁷ JP 3-09, III-13; JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017, Incorporating Change 1, October 22, 2018), III-37, available at <https://irp.fas.org/doddir/dod/jp3_0.pdf>.
- ¹⁸ Research Task Group SAS-151, "Solutions Enabling Intermediate Force/Non-Lethal Weapon Contributions to Mission Success," video, 2:37, March 30, 2022, available at <<https://www.youtube.com/watch?v=m7OPzalSb9w>>.
- ¹⁹ *Multi-Service Tactics, Techniques, and Procedures for the Employment of Nonlethal Weapons*, 2.
- ²⁰ Wendell B. Leimbach, Jr., "DOD Intermediate Force Capabilities: Bringing the Fight to the Gray Zone," Joint Intermediate Force Capabilities Office, available at <https://jnlwp.defense.gov/Portals/50/Documents/Resources/Presentations/IFCOOverviewBrief_CoLL_short>.
- ²¹ AJP-3.10, I-2.
- ²² JP 3-13, *Information Operations* (Washington, DC: The Joint Staff, November 27, 2012, Incorporating Change 1, November 20, 2014), GL-3, available at <https://irp.fas.org/doddir/dod/jp3_13.pdf>.
- ²³ AJP-3.10, I-10; JP 3-12.
- ²⁴ JP 3-13, II-6.
- ²⁵ AJP-3.10, 1-3.
- ²⁶ JP 3-0, xiii.
- ²⁷ *Ibid.*, IV-1–IV-2.
- ²⁸ Susan LeVine, "Beyond Bean Bags and Rubber Bullets: Intermediate Force Capabilities Across the Competition Continuum," *Joint Force Quarterly* 100 (1st Quarter 2021), available at <<https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497112/beyond-bean-bags-and-rubber-bullets-intermediate-force-capabilities-across-the/>>.
- ²⁹ JP 3-85, *Joint Electromagnetic Spectrum Operations* (Washington, DC: The Joint Staff, May 22, 2020), I-1, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf>.
- ³⁰ *Ibid.*, I-13.
- ³¹ *Ibid.*, I-2.
- ³² *Ibid.*, I-5.
- ³³ "NATO MC 64/11 Electronic Warfare Policy," July 2018, quoted in Malte von Spreckelsen, "Electronic Warfare—The Forgotten Discipline," *The Journal of the Joint Air Power Confidence Centre* 27 (Autumn/Winter 2018), available at <<https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/>>.
- ³⁴ *Ibid.*, 2.
- ³⁵ JP 3-85, B-1.
- ³⁶ JP 3-12, I-1, II-11.
- ³⁷ *Ibid.*, I-1.
- ³⁸ *Ibid.*, ix.
- ³⁹ *The Warsaw Declaration on Transatlantic Security*, NATO, July 9, 2016, available at <https://www.nato.int/cps/en/natohq/official_texts_133168.htm>.
- ⁴⁰ Martin C. Libicki and Olesya Tkacheva, "Cyberspace Escalation: Ladders or Lattices?" in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, ed. A. Ertan et al. (Tallinn, Estonia: NATO Cooperative Cyber Defense Centre of Excellence, 2020), 70, available at <<https://ccdcoc.org/uploads/2020/12/Cyber-Threats-and-NATO-2030-Horizon-Scanning-and-Analysis.pdf>>.
- ⁴¹ George Perkovich and Ariel E. Levite, ed., *Understanding Cyber Conflict: Fourteen Analogies* (Washington, DC: Georgetown University Press, 2017), 3.
- ⁴² *Ibid.*
- ⁴³ Robert E. Schmidle, Jr., Michael Sulmeyer, and Ben Buchanan, "Nonlethal Weapons and Cyber Capabilities," in Perkovich and Levite, *Understanding Cyber Conflict*, 31.
- ⁴⁴ David B. Law, "Directed Energy (DE) Intermediate Force Capabilities (IFCs): Relevant Across the Range of Military Operations," PowerPoint presentation, Joint Intermediate Force Capabilities Office, Quantico, VA, January 27, 2021, available at <<https://jnlwp.defense.gov/Portals/50/Documents/Resources/Presentations/DSIAC-Webinar-DE-Intermediate-Force-Capabilities.pdf?ver=nIDCf75TAytk16Je3N5hkg%3d%3d>>.
- ⁴⁵ *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 90, available at <https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf>.
- ⁴⁶ Yasmin Tadjeh, "Directorate Wants to Change View of Nonlethal Weapons," *National Defense*, July 31, 2019, available at <<https://www.nationaldefensemagazine.org/articles/2019/7/31/directorate-wants-to-change-view-of-nonlethal-weapons>>.
- ⁴⁷ Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 87.
- ⁴⁸ *Future of Defense Task Force Report 2020* (Washington, DC: House Armed Services Committee, September 23, 2020), 20.
- ⁴⁹ *Intermediate Force Capabilities*, 1.
- ⁵⁰ *Advantage at Sea*, 18.
- ⁵¹ David H. Berger, "A Message from the Commandant of the Marine Corps," March 6, 2022, available at <<https://mca-marines.org/wp-content/uploads/FMFMI-Warfighting-Anniversary-Letter-from-CMC.pdf>>.



Sergeant Adam Dorian Wong, threat researcher with 136th Cybersecurity Unit, presents new topics of interest including artificial intelligence and vulnerability identification to Salvadoran cyber security unit in El Salvador, December 7, 2022 (U.S. Air National Guard/Victoria Nelson)

The New “Cyber” Space Race

Integrating the Private Sector Into U.S. Cyber Strategy

By Natalie R. Alen, Gregory M. Eaton, and Jaime L. Stieler

Lieutenant Natalie R. Alen, USMCR, is the Programs and Data Officer in Charge, Reserve Affairs Division, Manpower and Reserve Affairs. Captain Gregory M. Eaton, SC, USNR, is the Joint Directorate Chief, Defense Logistics Agency Distribution Joint Reserve Force. Colonel Jaime L. Stieler, USAF, is Director of Operations, 480th Intelligence, Surveillance, and Reconnaissance Wing.

Current Russian cyber warfare capability demonstrates that nation’s growing sophistication with integrating cyberpower across the whole of society as a fully fledged instrument of national power. Russia’s cyber activities have blended kinetic action with escalated information

domain attacks to wage ongoing, low-intensity offensive campaigns that the U.S. military refers to as *hybrid warfare*. The Russian military’s integration of cyber with other “patriotic” nonstate actors includes the use of hackers and criminal organizations suspected of being directly linked

to or controlled by Russian security services. James Wirtz notes, “Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives.”¹

The impact of Russia’s rise as a cyberpower and the Kremlin’s use of cyber warfare as an instrument of power have not gone unnoticed by U.S. Government and military leaders. The

questions remain, however: What can the United States learn from Russia, and how has the United States adapted its national strategy for cyberpower to this integrated, whole-of-society approach to international competition and conflict? In *Cyberpower and National Security*, Franklin Kramer, Stuart Starr, and Larry Wentz assert:

Cyberpower is now a fundamental fact of global life. In political, economic, and

*military affairs, information and information technology provide and support crucial elements of operational activities. U.S. national security efforts have begun to incorporate cyber into strategic calculations. Those efforts, however, are only a beginning. The critical conclusion . . . is that the United States must create an effective national and international strategic framework for the development and use of cyber as part of an overall national security strategy.*²



Members of 169th Cyber Protection Team and members of Armed Forces of Bosnia and Herzegovina conduct cyber adversarial exercises at Private Henry Costin Readiness Center in Laurel, Maryland, June 29, 2022 (U.S. Army National Guard/Tom Lamb)

While the U.S. Government works to decrease the Nation's vulnerability to cyber attacks by improving network security and resiliency, it is time to start integrating the private sector as part of a larger information domain strategy for developing U.S. cyber advantage. As the Kremlin becomes more sophisticated in developing and using cyber warfare, the United States must also be able to mobilize a whole-of-society approach to integrate private- and public-sector capabilities, including U.S. military expertise, to compete and win in this new era of great cyberpower competition. Still, private-sector resistance to information-sharing and collaboration with the U.S. Government remains an obstacle to implementing a successful national cyber strategy. To overcome this, government leaders should examine the last time the United States faced a new and emerging domain of international competition for creating a successful integrated public-private-military organization for exercising national power.

Origins of Russian Integrated Cyberpower

Russian cyber attacks, including distributed denial-of-service (DDoS) attacks and attacks on critical infrastructure and networks, have been widely reported in the press for many years. These attacks and intrusions by ostensible nonstate actors are suspected of being directed and controlled by the Kremlin. In 2007, Russia's Federal Security Service was believed to be behind DDoS attacks on banks, media outlets, and government bodies in Estonia, which may have constituted the first use of cyberwarfare as a coercive tool to exercise political influence.³

In 2008, Russian-affiliated groups, including the criminal gang known as the Russian Business Network, disrupted Georgian government communications, banks, transportation companies, and telecommunications providers in advance of a Russian ground invasion.⁴ In addition, Russian "hactivist" Web sites published lists of Georgian sites for other hackers to target, including instructions and downloadable malware.⁵ Russia's

Ministry of Defense subsequently created a formal branch responsible for information operations, effectively integrating military capabilities and nonstate actors under a whole-of-society umbrella for cyber and influence operations.

Moscow's malign cyber activities are ongoing, and their proven approach to advancing the Kremlin's interests using cyberwarfare as an instrument of national power presents a significant challenge to the United States in great cyberpower competition.

Lessons from the Kremlin

Perhaps the most important lesson to learn from Russia's use of integrated cyberwarfare is not technical, but organizational: the use of a single coordinating authority to effectively integrate Russian state, military, and nonstate actor capabilities across the full spectrum of information operations. According to CNA, Russian military theorists do not even use the term *cyberwarfare*.⁶ Instead, cyber operations are considered part of the broader term *information warfare*, which Moscow views as a means for

*enabling the state to dominate the information landscape . . . and is to be employed as part of a whole of government effort, along with other, more traditional, weapons of information warfare that would be familiar to any student of Russian or Soviet military doctrine, including disinformation operations, [psychological operations], electronic warfare, and political subversion.*⁷

This viewpoint is echoed by author Yavor Raychev, who highlights key differences in the concepts of cyberwarfare in Russian and American politico-military thought.⁸ According to Raychev, Americans view cyberwarfare as a part of modern hybrid war, which blends conventional warfare, irregular warfare, and cyberwarfare.⁹ But as Raychev points out, "In the Russian tradition, before the disintegration of [the Soviet Union], 'hybrid war' referred rather to *political and information operations*."¹⁰ This raises the question of what the U.S. Government's

strategic approach should be to integrate the information domain as an instrument of cyberpower, incorporating U.S. military and private-sector capabilities.

Current U.S. Cyber Strategy and Public-Private Partnerships

Public-private partnerships between industry and the U.S. Government around cyber protection and initiatives began during the Bill Clinton administration, and they continue to expand.¹¹ Whereas the Russian military has employed criminal nonstate actors to augment and execute its cyber capabilities, the United States has leveraged the talent and expertise of respected U.S.-based firms to collaborate on cybersecurity for critical infrastructure in the public and private sectors. The 2018 National Cyber Strategy calls for "technical advancements and administrative efficiency across the Federal Government and the private sector" to secure cyberspace.¹² Similarly, the 2018 Department of Defense (DOD) Cyber Strategy identifies the need to increase the resilience of U.S. critical infrastructure through interagency and private-sector partnerships.¹³ The Department of Homeland Security (DHS) leads this effort through the Cybersecurity and Infrastructure Security Agency (CISA) to build stronger defense and resilience through public-private partnerships.¹⁴ For example, CISA oversees information-sharing programs, such as sector-specific Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). These nonprofit, member-driven organizations have been formed by private-sector critical infrastructure owners to gather, analyze, and disseminate cyber threat information between government and industry in order to promote better cybersecurity information-sharing and enhance collaboration and information-sharing among the private sector.¹⁵

While these partnerships have succeeded in improving U.S. cyber defenses, there are calls for greater integration between government and private-sector corporations to further develop

U.S. cyber capabilities for the private, civil, and defense sectors. For the past several years, General Paul Nakasone, commander of U.S. Cyber Command (USCYBERCOM) and director of the National Security Agency (NSA), has actively pursued partnerships with technology companies, emphasizing that the private sector and Silicon Valley are at the forefront of innovative thinking.¹⁶

Former USCYBERCOM commander and NSA director Admiral Mike Rogers argues that the United States is not taking an optimal approach when it comes to government and private-sector relations. Currently, we are collaborating in a manner wherein the public and private sectors are internally focused and inform one another if something relevant is discovered. Admiral Rogers advocates that the United States should move beyond collaboration and into integration, where the government and private sector work together around the clock on cybersecurity in a mutually beneficial partnership.¹⁷ Integrated partnerships between the government and private-sector tech companies signal momentum toward strengthening alliances and attracting new partnerships, one of the strategic lines of effort in the 2018 DOD Cyber Strategy.¹⁸

The strategy calls for greater sharing of information among allies and other key partners to enhance the effectiveness of collective cyber operations and to build trusted private-sector partnerships. While the strategy promotes information-sharing, concerns remain over the speed with which information is shared and declassified for use. In a memorandum to the Director of National Intelligence, several combatant commanders raised concerns about the inability to share and circulate overly classified intelligence regarding adversary behaviors and receiving intelligence too late.¹⁹ The memo depicts significant challenges in information-sharing with the interagency, allies, and key partners. If the United States aims to advance government and private-sector partnerships to leverage the innovations of Silicon Valley, the speed and scope of information being shared will require a more progressive approach.

Big Tech, the U.S. Military, and the Information Domain

In the United States, most cyber architecture, operations, and expertise reside in the civilian marketplace.²⁰ Despite this, the current U.S. approach to cyber operations does not effectively integrate private-sector expertise. To compete successfully against Russia's authoritarian system, a balanced whole-of-society approach is needed that is both reflective of our democratic values and effective against our adversaries. As noted by Raychev, "It can be concluded that the Western view on cyberwar is predominantly military-focused and technocratic. It views cyberwar in the broader context of cyber conflict as a modern form of fighting, but hardly grasps its social dimensions."²¹ While experts can disagree with Raychev on the U.S. Government's understanding of the full context of cyber interactions, it is evident that gaps exist between this military view of cyber operations and the untapped civilian resources that do not integrate well with the military-minded approach.

Joint Publication (JP) 5-0, *Joint Planning*, codified the Chairman of the Joint Chiefs of Staff's recognition that successful use of military power in support of U.S. interests is coordinated closely with the other three instruments of national power: diplomatic, informational, and economic.²² Interagency coordination among what is known as the "3Ds"—diplomatic, development, and defense establishments for planning and conducting operations—is a critical element of U.S. engagement policy and success. Exploring the concept of greater integrated public-private partnerships in the information domain through interagency coordination has increased applicability to the new era of cyber competition and operations.

The principles of interagency cooperation are outlined in military doctrine such as JP 5-0, and the National Security Council continues to facilitate the "mutual understanding and cooperation" necessary to achieve unity of effort in wielding all instruments of national

power.²³ However, big tech firms have been reluctant to fully collaborate with the U.S. Government on cyber issues. This inhibits a unity of effort between public- and private-sector entities for use of, and protection within, the cyber realm. As noted by Darko Trifunović, leading tech corporations exposed by the Edward Snowden leaks as engaging in U.S. cyberpower missions reacted by distancing themselves from "political subordination or participation in the national distribution of cyber war."²⁴ In addition, some private-sector firms have turned away from national cybersecurity protection programs and have opted to look for alternate solutions of their own to provide cyber protection. According to the Carnegie Endowment for International Peace, "the more resourceful and sophisticated private sector entities are scaling up their own efforts to address cyber threats. In addition to a range of security measures, many have turned increasingly to the risk challenging mechanism offered by cyber insurance policies. Yet the cyber insurance coverage presently available provides only a limited, uncertain, and ad hoc solution."²⁵

The stand-up of CISA in 2018 as an independent Federal agency under DHS, similar to the Federal Emergency Management Agency, was an attempt by the U.S. Government at creating a single organization responsible for integrating cybersecurity across the Federal civilian agencies and to provide for greater public-private cooperation on protecting critical infrastructure networks.²⁶ Since its inception, however, CISA has been widely criticized by privacy advocates and big tech companies, such as Apple and Amazon, for allowing data to be shared with other companies and the U.S. Government.²⁷ An internal DHS Office of the Inspector General report concluded that improvements in data-sharing are still needed.²⁸ A May 12, 2021, executive order on improving the Nation's cybersecurity was aimed at addressing the need for greater information-sharing among departments and agencies and the private sector, but issues still remain between CISA and the private sector over privacy and collaboration.²⁹



Participants analyze metadata to identify any suspicious activity on network during 2-week cyber exercise Tacet Venari, at Ramstein Air Base, Germany, May 12, 2022 (U.S. Air Force/Jared Lovett)

A Digital Arm for U.S. Cyber Integration

A potential solution for integrating the private sector into U.S. cyberpower strategy could be adding a fourth pillar—*digital*—to the 3Ds for protecting U.S. national security in the information domain. A new fourth “D” could serve to broker cyber information and innovation from big tech companies with the cyber defense and operations capabilities of the government and the U.S. military while still preserving the independence

of the private sector. Akin to how the U.S. Agency for International Development operates as lead for the *development* arm of the 3Ds of U.S. foreign policy, an independent, civilian-led agency could drive U.S. cyber interests and economic prosperity in the information domain by using partnerships and investments that protect critical infrastructures. A new D agency could also serve as a conduit for Federal research and development in cyber technology and technology transfer programs. A similar model of public-private

partnerships was adopted during the Cold War period with the creation of agencies such as the National Science Foundation and the Defense Advanced Research Projects Agency. Federal funding for research and development resulted in the creation of new scientific and technical capabilities leading to the establishment of new industries, benefiting both the Federal Government and the private sector.³⁰ A similar leading digital pillar of government would not only sustain investment and innovation

in the information domain but also strengthen the other instruments of national power and provide the organizing energy needed to maximize U.S. public-private coordination in great cyberpower competition with Russia.

The concept of a truly integrated fourth D, or digital arm, would also require the ability to ensure separation between civilian and military activities within the competition continuum.³¹ As demonstrated in the 2018 petition by 4,000 Google employees who demanded “a clear policy stating that neither Google

nor its contractors will ever build warfare technology,” many within the U.S. cyber technology field are uncomfortable with working toward a U.S. cyber advantage if it means working in direct support of DOD objectives.³² Furthermore, controversy remains over the law of armed conflict principle of *distinction* as applied to civilians participating in direct hostilities in the information domain.³³ A digital arm of what would become the 4Ds would need to provide the necessary privacy, oversight, and coordination among all U.S. cyber technology activities. At

the same time, it also should build clear distinctions between civilian capabilities and government or military objectives and position the United States to better engage in an open whole-of-society approach to compete against Russia and other nation-states in the information domain. Such an organization further would need authority to develop incentives for private-sector firms to overcome privacy and data-sharing concerns, such as grants, limited liability protections, and access to cybersecurity research, to name a few.³⁴



Sergeant Ian McConnell, cyber warfare operator for Defensive Cyberspace Operations–Internal Defensive Measures, 8th Communication Battalion, works on his network hacking plans during Cyber Yankee 22, on Camp Nett, Niantic, Connecticut, June 13, 2022 (U.S. Marine Corps/Ashley Corbo)

Integrating the Information Domain

Establishment of a fourth D organization to integrate government and private-sector activities while keeping civilian and military objectives separate is needed for achieving unity of effort in the era of great cyberpower competition. According to one article:

Governments have a unique capacity to facilitate information sharing and engagement. Doing so would help rebuild the relationships among the innovation triangle—the public sector, private industry, and academia—and would encourage mutual understanding, a necessary step for breaking down the cultural barriers that restrict collaboration between government and high-tech firms.³⁵

Fortunately, a template for this very type of organization was designed by the U.S. Government more than 60 years ago in response to another national security domain challenge stemming from Russia. In 1957, the Soviet Union launched its first satellite—Sputnik. This triggered what came to be known as the space race and drove the need for the United States to rapidly mobilize both government and private-sector capabilities into the space domain.³⁶ The National Aeronautics and Space Administration (NASA) was thus created in 1958 and continues to oversee America’s space program, integrating civilian and military capabilities. The National Aeronautics and Space Act, the legislation that created NASA, “allow[ed] the agency to enter into contracts with industry and educational institutions and call[ed] for the widest possible practicable and appropriate dissemination of information.”³⁷ Quoting directly from the original act, Sec. 103, paragraph b:

The Congress further declares that such activities [aeronautical and space] shall be the responsibility of, and shall be directed by, a civilian agency exercising control over aeronautical and space activities sponsored by the United States, except . . . activities peculiar to or primarily associated with the development of weapons systems, military operations, or defense of the United States.³⁸

This type of legislation and organizational arrangement echoes the calls by General Nakasone and Admiral Rogers for providing greater integration and information-sharing with the private sector in the information domain, while separating the private sector from any military cyber activities conducted by USCYBERCOM or other DOD entities.

Extreme Makeover: CISA Edition

At its creation, CISA may have been imagined as a NASA-like solution; however, in its initial 4 years of existence, it has yet to capture the public imagination or energize the private sector in the same way as NASA did. Early challenges with managing data privacy and data-sharing have undercut CISA’s effectiveness in fully integrating the private sector into U.S. cyber strategy. For CISA to become the digital organization to integrate government and private-sector efforts across cyber, it would benefit from following the same path as NASA.

A first step would be decoupling CISA from DHS to give the agency more operational independence and to increase the agency’s visibility and public profile as the U.S. Government’s face, or digital arm, for cyber security. Former head of CISA, Christopher Krebs, has publicly advocated for CISA breaking out from DHS and becoming a stand-alone agency to give the private-sector and other stakeholders a clearly visible “front door” for working with the government to combat cyber threats.³⁹

Second, CISA should be invested with greater budget authorities for sponsoring cyber research and development and for incentivizing private-sector participation through contracting and grants. Although CISA currently oversees industry forums for sharing information on protecting critical infrastructure, such as the ISACs and ISAOs, participation and membership are strictly voluntary, and CISA offers only programmatic support. A new fiscally empowered CISA could continue to manage and leverage these existing relationships while being able to

incentivize greater participation through access to grant programs and research and development funding.

Finally, a newly independent and rebranded CISA could serve as a “cyber center of excellence” by collecting and promulgating cyber information, cyber expertise, and best practices from government, academia, and the private sector, while keeping offensive cyber objectives separated. This reimagined CISA could serve as a magnet for developing U.S. cyber talent by not only increasing its existing training offerings but also creating internships, sabbatical opportunities, research assistantships, and funded executive-in-residence programs with tech companies to accelerate the growth of cyber talent both for the U.S. Government and industry. Rotational assignment opportunities with other governmental agencies and the military departments could also serve to “cross-pollinate” talent and build professional networks needed to achieve the unity of effort required for great cyberpower competition.

Today, much of the U.S. cyber talent and capabilities reside in the private sector. A successful national cyberpower strategy must be able to integrate these resources, as Russia has effectively demonstrated, while maintaining our uniquely American character. An organized and flexible integration of government and private-sector tech capabilities in the United States requires an approach that facilitates information-sharing and unity of effort in support of national interests while at the same time protecting privacy concerns and maintaining the freedom of association foundational to American values. The reinvention of CISA into a NASA-like organization responsible for integrating public- and private-sector activities on the development and use of cyber provides the potential means for establishing a unity of effort between the government and the private sector. This would allow the U.S. Government to employ a whole-of-society approach while ensuring private-sector cyber tech companies can maintain separation from direct hostilities within the information domain. JFQ

Notes

¹ James J. Wirtz, “Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy,” in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 31, available at <https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf>.

² Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC: NDU Press, 2009).

³ Michael Connell and Sarah Vogler, *Review of Russia's Approach to Cyber Warfare* (Arlington, VA: CNA, September 2016), 13, available at <<https://apps.dtic.mil/sti/pdfs/AD1019062.pdf>>.

⁴ John Markoff, “Before the Gunfire, Cyberattacks,” *New York Times*, August 12, 2008; Connell and Vogler, *Review of Russia's Approach to Cyber Warfare*, 18.

⁵ Connell and Vogler, *Review of Russia's Approach to Cyber Warfare*, 17.

⁶ *Ibid.*, 3.

⁷ *Ibid.*

⁸ Yavor Raychev, “Cyberwar in Russian and U.S.A. Military-Political Thought: A Comparative View,” *Information & Security: An International Journal* 43, no. 3 (2019), 354.

⁹ *Ibid.*, 351.

¹⁰ *Ibid.*, 349. Emphasis added.

¹¹ Madeline Carr, “Public-Private Partnerships in National Cyber-Security Strategies,” *International Affairs* 92, no. 1 (2016), 43–62.

¹² *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 21, 2018).

¹³ *Department of Defense Cyber Strategy* (Washington, DC: Department of Defense [DOD], September 2018).

¹⁴ “Protecting Critical Infrastructure,” Cybersecurity and Infrastructure Security Agency (CISA), September 7, 2021, available at <<https://www.cisa.gov/protecting-critical-infrastructure>>.

¹⁵ “Information Sharing and Awareness,” CISA, February 16, 2022, available at <<https://www.cisa.gov/information-sharing-and-awareness>>.

¹⁶ Mark Pomerleau, “U.S. Cyber Command's Top General Makes Case for Partnering With Tech Firms,” *C4ISRNET*, August 25, 2020, available at <<https://www.c4isrnet.com/cyber/2020/08/25/us-cyber-commands-top-general-makes-case-for-partnering-with-tech-firms/>>.

¹⁷ Ryder Ashcraft, “Admiral Mike Rogers, USN (Ret.),” *DOD Reads: What Are You Reading?* podcast, April 26, 2021, available at <<https://anchor.fm/dodreads/episodes/Admiral-Mike-Rogers--USN-Ret-ubfn6>>.

¹⁸ *Department of Defense Cyber Strategy*.

¹⁹ Betsy Woodruff Swan and Bryan Bender, “Spy Chiefs Look to Declassify Intel After Rare Plea from 4-Star Commanders,” *Politico*, April 26, 2021, available at <<https://www.politico.com/news/2021/04/26/spy-chiefs-information-war-russia-china-484723>>.

²⁰ Max Smeets, “U.S. Cyber Strategy of Persistent Engagement and Defend Forward: Implications for the Alliance and Intelligence Collection,” *Intelligence and National Security* 35, no. 3 (2020), 450.

²¹ Raychev, “Cyberwar in Russian and U.S.A. Military-Political Thought,” 353.

²² Joint Publication 5, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), xv, available at <https://irp.fas.org/doddir/dod/jp5_0.pdf>.

²³ *Ibid.*, I-24.

²⁴ Darko Trifunović and Zoran Bjelica, “Cyber War—Trends and Technologies,” *National Security and the Future* 21, no. 3 (2021), 76, available at <<https://doi.org/10.37458/nsf.21.3.2>>.

²⁵ Ariel E. Levite, Scott Kannry, and Wyatt Hoffman, *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance* (Washington, DC: Carnegie Endowment for International Peace, October 2018), available at <https://carnegieendowment.org/files/cyber_insurance_formatted_final_web.pdf>.

²⁶ Cynthia Brumfield, “What Is the CISA? How the New Federal Agency Protects Critical Infrastructure,” *CSO Online*, July 1, 2019, available at <<https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html>>.

²⁷ Graeme Caldwell, “Why You Should Be Concerned About the Cybersecurity Information Sharing Act,” *TechCrunch*, February 7, 2016, available at <<https://techcrunch.com/2016/02/07/why-you-should-be-concerned-about-cisa/>>.

²⁸ Jordan Smith, “CISA Aims to Improve Cyber Threat Data Sharing Problem,” *MeriTalk*, October 9, 2020, available at <<https://www.meritalk.com/articles/cisa-aims-to-improve-cyber-threat-data-sharing-program/>>.

²⁹ “Executive Order on Improving the Nation's Cybersecurity,” The White House, May 12, 2021, available at <<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>>.

³⁰ David H. McCormick, Charles E. Luftig, and James M. Cunningham, “Economic Might, National Security, and the Future of American Statecraft,” *Texas National Security Review* 3, no. 3 (Summer 2020), 56, available at <<https://tnsr.org/2020/05/economic-might-national-security-future-american-statecraft/>>.

³¹ Joint Doctrine Note I-19, *Competition Continuum* (Washington, DC: The Joint Staff,

June 3, 2019), 2–3, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.

³² Scott Shane and Daisuke Wakabayashi, “‘The Business of War’: Google Employees Protest Work for the Pentagon,” *New York Times*, April 4, 2018.

³³ David Wallace, Shane Reeves, and Trent Powell, “Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines,” *Harvard National Security Journal* 12 (2021), 186, available at <<https://harvardnsj.org/wp-content/uploads/sites/13/2021/02/HNSJ-Vol-12-Wallace-Reeves-and-Powell-Direct-Participation-in-Hostilities-in-the-Age-of-Cyber.pdf>>.

³⁴ Michael Daniel, “Incentives to Support Adoption of the Cybersecurity Framework,” Department of Homeland Security, August 6, 2013, available at <<https://www.dhs.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework>>.

³⁵ McCormick, Luftig, and Cunningham, “Economic Might, National Security, and the Future of American Statecraft,” 58.

³⁶ “The Birth of NASA,” National Aeronautics and Space Administration, March 28, 2008, available at <https://www.nasa.gov/exploration/whyweexplore/Why_We_29.html>.

³⁷ W.D. Kay, *Defining NASA: The Historical Debate Over the Agency's Mission* (Albany: State University of New York Press, 2005), 6.

³⁸ *National Aeronautics and Space Act of 1958*, H.R. 12875, Pub. L. 85-568, 85th Cong., 2nd sess., July 29, 1958, available at <<https://history.nasa.gov/spaceact.html>>.

³⁹ Suzanne Smalley, “Ex-CISA Chief Krebs Advocates for Standalone Cyber Agency. Experts Say That's Impractical,” *Cyberscoop*, August 12, 2022, available at <<https://www.cyberscoop.com/cybersecurity-experts-say-cisa-cannot-stand-alone/>>.

The Passage of the Delaware, by Thomas Sully, 1819, oil on canvas, Museum of Fine Arts Boston



General George Washington

First in War, First in Peace, First in National Security Strategy

By David C. Arnold

On July 4, 1776, American leaders at the Second Continental Congress terminated the strategy they had been executing

against Great Britain for over a year. They wanted political, military, and economic independence for the 13 colonies. To achieve that end, they relied

on all four instruments of national power—diplomatic, informational, military, and economic. But while many of the founders understood one or perhaps two of these instruments, General George Washington was the first American to execute a strategy using all four to achieve his ends—all

Colonel David C. Arnold, USAF (Ret.), Ph.D., is a Professor of National Security Strategy in the National War College at the National Defense University.

while operating in a joint, interagency, intergovernmental, and multinational (JIIM) environment, as complicated in its time as ours is today.

Long before he became President, Washington was a national security strategist who, as commander of all U.S. forces during the American Revolution, understood how all four instruments of national power could be orchestrated to achieve the aim of independence from Great Britain. Washington was undoubtedly the first and possibly the only officer to simultaneously serve as de facto Chairman of the Joint Chiefs, Chief of Staff of the Army, and commander of an army in a combat theater. His command of all the instruments of national power most certainly provides a superlative model for officers who will serve in the JIIM environment in the future.

According to Lieutenant General Dave R. Palmer, historian and former West Point superintendent, strategy was not a commonly used word until Carl von Clausewitz analyzed the Napoleonic Wars of the 19th century. Palmer argued that it “was not a word George Washington ever used.”¹ However, as Palmer also states, there was most certainly strategy before Clausewitz. In the 18th century, for the most part, a strategy meant “the rules of the game”—that is, maxims on how to execute battles, in much the same way Sun Tzu or Baron Antoine-Henri Jomini handed us recipes for success.² For military officers, the word strategy referred then to military tactics, not national security strategy or even grand strategy. What today we would call “national security strategy” or “grand strategy” was only for kings and their ministers.

Complicating matters, the new United States did not have a modern national leadership structure during the American Revolution. It was not until 1781 that the 13 new states even ratified the Articles of Confederation, under which each state acted as a sovereign nation. (The Constitution that we operate under today was still several years into the future.) Ideas about national-level strategy fell to the delegates to the Second Continental Congress—among whom

Washington was counted from the spring of 1775 until he became commander of the Continental Army. At that point, with the Declaration of Independence still a year away, ideas about military strategy—that is, tactics—fell on the shoulders of the new and unanimously elected commander in chief of the Continental Army, George Washington.³

Washington’s military career embodies many of the goals set out in current-day military education. In the most recent Chairman of the Joint Chiefs Instruction on joint professional military education (JPME), the Chairman articulated his commander’s intent for JPME, which is “the development of strategically minded joint warfighters who think critically and can creatively apply military power to inform national strategy, conduct globally integrated operations, and fight under conditions of disruptive change.”⁴ After 1778, North America was a theater in a globally integrated operation between the British and French, in which Washington was the American theater joint commander and the combined forces commander for the allied American and French forces. He was very much a strategically minded critical thinker who learned from his mistakes and fought under conditions of highly disruptive change.

There are many vocabularies of and approaches to strategy, but this article uses standard definitions from *A National Security Strategy Primer* by the National War College’s Steven Heffington, Adam Oler, and David Tretler.⁵ This article uses a *Primer*-informed language and its common vocabulary to argue that Washington—because he was often on his own tactically, operationally, and strategically while acting as diplomat, intelligence chief, soldier, and economist—wielded the instruments of national power to achieve his ends in all the ways the *Primer* intended, more than 200 years before its publication. Today’s JPME is not trying to create an officer who can do all three of the jobs Washington did simultaneously, nor should it, but JPME students could do well to learn from Washington’s example since his

efforts led to victory. Strategically minded officers need to consider that the concept of national security strategy, according to the *Primer*, and as reflected in Washington’s actions, “can apply broadly, organizing or guiding nearly all aspects of a state’s policy, or more narrowly regarding a specific situation.”⁶

For most of his life, Washington was more citizen than soldier. Washington was not traditionally trained in the art of war like many of his peers who came up through the ranks in their national armies. He had received a commission as a major in the Virginia colonial militia from Lieutenant Governor Robert Dinwiddie in 1754, when Washington was just 22 years old. On his second mission for the Crown, Washington inadvertently started a world war when he participated in the death of a French envoy in a fire at Jumonville Glen, in what is now southern Pennsylvania, igniting the Seven Years’ War (known in the colonies as the French and Indian War). After adventures during the 1750s with two different British generals, finding himself unable to secure a commission in the regular army, and newly married, Washington left military service in 1758 to spend his days as a member of Virginia’s land-holding class. During this time, he was often referred to as “Colonel Washington.”⁷ By the time of the Second Continental Congress in 1775, he had achieved military and political notoriety in the colonies. John Adams recalled years later that he suggested Washington for leadership of the Continental Army because Washington was “a Gentleman whose Skill and Experience as an Officer, whose independent fortune, great Talents and excellent universal Character, would command the Approbation of all America, and unite the cordial Exertions of all the Colonies better than any other Person in the Union.”⁸

Therefore, Washington’s professional military education consisted of what he had learned on the job, his time as part of the military “families” of more senior officers during the French and Indian War, and his wide reading of books on military tactics. He read Humphrey Bland’s *Treatise of Military Discipline* in the 1750s and, when asked, would



Portrait of George Washington,
by Charles Willson Peale, 1772,
oil on canvas, Washington and
Lee University



General George Washington Resigning His Commission, by John Trumbull, 1817–1824, oil on canvas, U.S. Capitol rotunda (Architect of the Capitol)

recommend books to fellow officers during the war.⁹ But he did not attend military academies or schools, and when his father passed away, his older brother Lawrence did not send young George to attend school in Great Britain as had been Washington family tradition. Washington was tutored for a time as a young man, though his formal schooling eventually stopped and never included the military arts and sciences. By the time Congress elected Washington commander in chief, he had been out of the formal British military system for over a decade.¹⁰ (It was in the buff and blue uniform of the independent Fairfax County militia, formed in 1774, that Washington attended the Second Continental Congress in 1775.)

Washington had not been the only choice for commander in chief that year. Also considered were New Englander John Hancock, then president of the Continental Congress and a wealthy

merchant, and former British officers Charles Lee and Horatio Gates, who both had considerably more military experience than Washington. Washington was chosen for many reasons: his lack of outwardly expressed desire for the role, his wealth, his renown in the colonies, and the simple fact that he was not a New Englander. Congress chose Washington, who took the job while feeling “great distress” because he feared his own “abilities & Military experience may not be equal to the extensive & important Trust.”¹¹ He was appointed a senior government leader and, therefore, also a national security strategist.

Washington began his command by defining a problem and an end to achieve, aware of the resources at his disposal. The short-term end was to eject the British from Boston, which the combined armies did with their siege of the city in the winter of 1775–1776. With the Declaration of Independence in the summer of 1776,

Washington gained a much clearer vision of what the national end looked like. From the beginning, he grasped the document’s importance, ordering it to be read aloud to the troops defending New York City.¹² Yet a key to strategic success for every national security strategist, regardless of an individual’s parent agency, is the “national” in national security strategy. Understanding the capabilities and limitations of the instruments of national power can help determine an effective solution to a national security problem, and by 1776, Washington had a big problem on his hands.

The Diplomatic Instrument.

Washington was not a true diplomat—he left that work to Thomas Jefferson and Benjamin Franklin, who served in Paris as the American envoys from Congress and negotiated the Franco-American alliance—but Washington did represent the United States as many military officers do

today in his relationship with the forces of our first ally, France. The *Primer* points out that the three ways in which strategists can wield the diplomatic instrument are through representation, negotiation, and implementation.¹³ Washington utilized all three. First, he represented the United States after the alliance with France as the leader of a military alliance. Historian Benjamin Huggins argues that Washington's "diplomatic skills proved critical to the preservation of the alliance in the face of military setbacks and to winning the confidence of French leaders."¹⁴ For example, after the arrival of the French navy in New England in the summer of 1778, Washington negotiated with Admiral Comte d'Estaing for an attack on Newport, Rhode Island, which the combined force undertook, though with little success.

With the arrival of more French forces in 1780, Washington worked with French General Comte de Rochambeau—who was told to recognize Washington as the overall combined force commander—to prepare an assault on New York City.¹⁵ By the time of the Wethersfield Conference in Connecticut in 1781, Washington was a military officer working with allies to achieve a common goal—defeating the British in North America. The alliance was finally cemented when combined American and French forces, agreeing that an attack on New York City would be unsuccessful, besieged and captured Yorktown, with support from the French navy. In the process, the allies defeated the British, taking over 8,000 British troops prisoner.

The Informational Instrument.

Washington was not a true intelligence professional, although he had part-time advisors on intelligence. Historian John Nagy explained that Washington was not only a reader of enemy orders of battle and troop movements but also a consumer of "open-source material such as gossip, rumors, newspapers," and information gleaned from British deserters.¹⁶ The *Primer* points out that the three ways in which strategists can wield the information instrument are by perceiving, informing, and manipulating.¹⁷ In his time, Washington was able

to collect, process, integrate, analyze, and interpret the available strategic information he had.¹⁸

Yet he sometimes failed to achieve his goals in battle successfully. The Battle of Brandywine was a notorious tactical intelligence failure for Washington, according to historian Kenneth Daigler, who argued that "he and his officers were not familiar with the countryside where they would have to fight. . . . He only had an inaccurate map of the area, and despite his orders, the local military failed to conduct aggressive scouting of the British movements."¹⁹ The result was the worst defeat of the 1777 campaign. But Washington, who was in constant communication with Congress about the actions of the Continental Army and its needs, did inform Congress of the defeat, stating that the intelligence he had received "was uncertain & contradictory, notwithstanding all my pains to get the best."²⁰

Washington was also a master manipulator of information, whether hiding the amount of ammunition available for the Continental Army around Boston or using unmanned campfires to mask the movement of the Army at Princeton. He launched his "most important and comprehensive strategic deception operation of the war" in convincing the British that a combined Franco-American attack against New York was imminent in 1781, all the while moving the allies' armies to besiege Yorktown.²¹

Finally, Washington took great interest in the spy ring that his part-time intelligence chief Major Benjamin Tallmadge was running in the New York City area, even compartmentalizing the existence of the Culper Ring and providing Tallmadge clear guidance and prioritization on the ring's targets.²²

The Military Instrument.

Washington was obviously a warrior, albeit an unconventionally educated one. The *Primer* points out that the three ways in which strategists can wield the military instrument are by using force, threatening to use force, and enabling the building of forces.²³ While over 230 skirmishes and battles were fought during the American Revolution, according to the digital encyclopedia of the

Fred W. Smith Library for the Study of George Washington at Mount Vernon, Washington was present for only 17 during the entire 1775–1783 war.²⁴ In fact, most of the battles he participated in took place from August 1776 to January 1777 (nine battles) and from September to December 1777 (four battles).

What was he doing the rest of the time as commander in chief? He was threatening to use force and building a new army. It was normal for armies of the 18th century to camp for the winter when the weather was cold and harsh and daylight minimal. The American Continental Army was no different in this regard. While the British army generally camped in American cities, quartering itself in local homes, the American army built small cities for itself. When the Continental Army pulled into Valley Forge for the winter of 1777–1778, it created the fifth-largest city in the 13 colonies. Washington chose Valley Forge based on critical strategic reasoning: its location was a natural fortress, close to Philadelphia, enabling the Army to deny the British access to forage outside the city, and it was between the British and the Continental Congress, which had evacuated Philadelphia for York, but not so close as to be an additional burden on the people of south-central Pennsylvania.²⁵ Similar reasons led to encampments at Morristown, New Jersey, and Newburgh, New York, both of which were close to New York City.

While at Valley Forge with the Army in winter quarters, Washington worked on creating a new American Army simply by doing his job as a staff officer. The result of this work was a 38-page memorandum to Congress that historian Edward Lengel called a "minor masterpiece of military administration" and that "ultimately laid the basis for victory at Monmouth and Yorktown."²⁶ Washington started by reminding Congress that while patriotic zeal was necessary, few men were capable of the continual sacrifice to conduct the war. He recommended a reorganization of the Continental Army. Whereas the 13 states had provided 97 regiments, none was at full strength by 1778; Washington

proposed reducing the number to 80. To make up for weak recruiting, he suggested drafting men from the militia units attached to the Continental Army, and to reduce disciplinary issues, he suggested creating the position of provost marshal. In addition, “He offered advice in his letter on reforming hospitals, redesigning the commissary [and] clothing and quartermaster departments; importing supplies from France; on Indian alliances; drill and training; camp sanitation; distributing liquor.” And as an illustration of Washington’s active participation in the human rights crime of American slavery, he also suggested conscripting slaves as wagon drivers.²⁷

The Continental Army needed to retain good officers, so Washington proposed a half-pay pension for those who stayed for the whole war, bonuses to those who remained at Valley Forge through the winter, and draft and reenlistment bonuses. He also suggested shrinking the Army and collapsing some units to make fewer, stronger ones, and reducing the numbers of staff officers by making some tasks additional duties.²⁸ In addition, Washington enlisted the assistance of an ex-Prussian soldier who trained the American Army to fight a European army with standardized European tactics.²⁹ When the Continental Army faced off against the British at the Battle of Monmouth in June 1778, which included nearly 30,000 soldiers, it was Britain’s turn to surrender the field.³⁰ Washington had coordinated his actions with Congress and the states and, with the addition of the French alliance in May 1778, successfully operated in the JIIM environment due to the new Army he had built.

The Economic Instrument. As a member of Virginia’s property-holding class, Washington lived within an economic system based on his enslavement of many men, women, and children. As part of this class, he certainly understood economic issues—even though he was not an economist. He understood that the nation’s economic capability was small—at a stage in which the mercantilist economic systems generally limited manufacturing to the mother country.

Historian Robert Middlekauff argued that by 1770, Washington, frustrated with the prices he was getting for his tobacco from his agent in London and the taxes imposed by Parliament, had begun to think about “resistance.”³¹

The *Primer* points out that the three ways in which strategists can wield the economic instrument for economic power are assistance, trade, and finance.³² From the beginning, Washington was aware of the military and economic means at his disposal, as when he wrote to his brother that Congress had just voted to provide \$2 million and 15,000 men for the Army.³³ Although the new nation’s economic capability was small, Washington wielded the economic instrument of power effectively when he could, and sometimes for multiple purposes. For example, at Valley Forge, the Continental Army was desperate for supplies. The Army had no meat in mid-December and only 25 barrels of flour for 14,000 men. Camp surgeon Dr. Albigence Waldo stated the men cried, “No meat! No meat!” sounding like “crows and owls.”³⁴ With Valley Forge at the center, the camp essentially stretched along an 80-mile-long crescent-shaped line from Wilmington (south of Philadelphia) to Trenton (north of Philadelphia), providing protection for the supply lines up the Chesapeake Bay and for the people in Delaware and New Jersey, and keeping the locals from trading with the British in Philadelphia.³⁵ As the Army and the local population foraged for supplies, they got in a bad way: Soldiers felt locals were holding on to too much, and they targeted the Quakers, calling them unpatriotic for being conscientious objectors.³⁶

In response, Washington established traveling markets that could both supply the Continental Army and preserve civil-military relations in the region outside Philadelphia.³⁷ The goal was to keep local merchants and farmers from crossing into the city to exchange goods for British silver and to improve relations with the locals. Washington publicly advertised the plan with assurances that there would be no commandeering of goods, carts, and wagons. But in February, the market system collapsed because of bad weather.

Washington was concerned that he faced a “fatal crisis, total want and dissolution of the Army” if things did not improve.³⁸ He eventually ordered his quartermaster, Major General Nathanael Greene, to strip the local countryside of supplies. Many locals hid their property because when Greene seized goods, he paid for them with “receipts” or destroyed them to keep them out of the hands of the British.³⁹ This led to Washington’s Army gaining more supplies but less civilian goodwill.⁴⁰ The locals “cry out and beset me from all quarters,” Greene wrote Washington on February 15, 1778, “but like Pharaoh, I harden my heart.”⁴¹ Washington had made a strategic decision to take what the Army needed. The results of these actions were providing supplies for the American Army and support for the American economy and currency, while simultaneously preventing the British from foraging in the area, which stressed their ocean-crossing supply lines even further.

Washington also believed he could assist in boosting the value of the new nation’s currency, called a “continental” and backed by the full faith but marginal credit of the United States, and which rose and fell with his success or defeat on the battlefield. A weak currency made it harder to supply the Continental Army, while a strong currency kept patriots from defecting to the British or trying to sell their goods for British silver.⁴² Washington also understood the benefits of assistance as an economic tool as his Army received both military and financial aid from France and supplies from France and the Netherlands.⁴³ Likewise, the bulk of the Yorktown campaign in fall 1781, which proved to be the decisive point of the war, was paid for with Spanish money that the French brought to the United States from Cuba.⁴⁴

Finally, Washington also understood the importance of finance. The Army faced constant funding issues throughout the war from a Congress that did not have the ability to tax the Nation but only to request funds from the individual states, which sometimes failed to pay their bills. Washington appealed directly to the governors of the various states to

support the troops they had raised and sponsored to be part of the Continental Army. Furthermore, much of the background to the Newburgh Conspiracy centered around the fact that the officer corps had not been paid in years; at that point, the promise made after Valley Forge of half-pay for an officer's life seemed a distant memory. Many officers planned to march on Congress at Philadelphia to demand their owed compensation with the threat of force. Washington's appeal to them in 1783 at the end of the revolution may have "saved the republic," historian William Fowler argued. In another scholar's mind, heading off a potentially violent march on Congress was a victory more complete than anything Washington won on the battlefield, well illustrating the importance of finance in war.⁴⁵

Washington saw things at the strategic, operational, and tactical levels because he was simultaneously commander of *the* Army and commander of

an army, which in modern terms meant he was both Chief of Staff of the Army and a theater commander, and eventually, after the French joined the war, a combined force commander. When the French brought to bear their significant naval power at Yorktown in 1781, Washington leaped at the opportunity to hand the British a decisive blow. He used his available means in myriad ways: he was not solely trying to eradicate his enemy—sometimes, he just needed to observe, accommodate, shape, persuade, enable, or induce the objects of his strategies to achieve his ends. He was a master orchestrator of the instruments of national power who used his limited available means to achieve national ends in clearly effective ways. The result speaks for itself: *independence*.

Washington's autodidactic success should not be misunderstood to mean that JPME is unimportant—absolutely not. In these times, self-study is no longer enough to achieve success, and

modern national security strategists must ask questions Washington never asked, such as, "What are the instruments of power?" and "How do you wield them?" In today's volatile, uncertain, complex, and ambiguous environment—one that functions under "conditions of disruptive change" and that is vastly more complicated and fast-moving than in the 18th century—we need a common understanding of strategic thinking and officers who understand the capabilities of all the instruments of national power, enabling them to be strategically minded and communicate effectively in the JJIM environment—that is, the same environment General Washington operated in over 200 years ago.

Washington's ability to craft effective strategy using all the instruments of national power was a hallmark of his military service and one we can do well to emulate. Undoubtedly, as President of the United States, George Washington was a national security strategist, whether



Scene at the Signing of the Constitution of the United States, by Howard Chandler Christy, 1940, oil on canvas, U.S. Capitol

it was in negotiating treaties, dealing with British forts on American territory, leading the military in difficult political times, or warning of entangling alliances as he left office. Indeed, as commander of the Continental Army, Washington may have been the first national security strategist, but he was certainly not the last officer the Nation needed to be among a group of “strategically minded joint warfighters who think critically and can creatively apply military power to inform national strategy, conduct globally integrated operations, and fight under conditions of disruptive change.”⁴⁶ We all should be. JFQ

Notes

¹ Dave R. Palmer, *George Washington’s Military Genius* (Washington, DC: Regnery Publishing, 2012), 1.

² *Ibid.*, 3.

³ “Address to the Continental Congress, 16 June 1775,” *Founders Online*, National Archives and Records Administration (NARA), available at <<https://founders.archives.gov/documents/Washington/03-01-02-0001>>. [Original source: *The Papers of George Washington*, Revolutionary War Series, vol. 1, 16 June 1775–15 September 1775, ed. Philander D. Chase (Charlottesville: University Press of Virginia, 1985), 1–3.] Even if Washington had wanted to turn to Clausewitz in some mythical universe in which Clausewitz wrote a draft of *On War* before the American Revolution, Clausewitz is so weak on “popular wars” that his treatise might not have been very useful. As Clausewitz put it, “it is possible to fight superbly, like men of the Vendée [who fought a 3-year, counter-revolution insurgency in western France in the 1790s that resulted in 240,000 killed—see David A. Bell, “The French Revolution, the Vendée, and Genocide,” *Journal of Genocide Research* 22, no. 1 (2020), 19–25] and to achieve great results, like the Swiss, the American, and even the Spaniards without developing the kind of virtues discussed here.” See Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 188. Unfortunately, when Clausewitz did write, 40 years after the American Revolution, he contributed little to discussions on wars of national liberation.

⁴ Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 1800.01F, *Officer Professional Military Education Policy* (Washington, DC: The Joint Staff, May 15, 2020), 1.

⁵ Steven Heffington, Adam Oler, and David

Tretler, *A National Security Strategy Primer* (Washington: NDU Press, 2019) (hereafter *Primer*).

⁶ *Ibid.*, 1.

⁷ For more on the early phases of Washington’s military career, any number of biographies are available. One of the best to focus on his early military career is Peter Stark’s *Young Washington: How Wilderness and War Forged America’s Founding Father* (New York: Ecco Press, 2018).

⁸ “Address to the Continental Congress, 16 June 1775,” n2.

⁹ John W. Hall, “An Irregular Consideration of George Washington and the American Military Tradition,” *Journal of Military History* 78, no. 3 (July 2014), 962; Oliver L. Spaulding, Jr., “The Military Studies of George Washington,” *The American Historical Review* 29, no. 4 (July 1924). Spaulding’s article is a brief look at the books on military topics in Washington’s personal library.

¹⁰ According to historian Jessica E. Brunelle, “In 1785 he referred to his education as ‘defective.’” See Jessica E. Brunelle, “The Youth of George Washington,” in *A Companion to George Washington*, ed. Edward G. Lengel (Hoboken, NJ: Wiley-Blackwell, 2012), 4.

¹¹ “Address to the Continental Congress, 16 June 1775.”

¹² Edward G. Lengel, *General George Washington: A Military Life* (New York: Random House, 2005), 136.

¹³ *Primer*, 14–15.

¹⁴ Benjamin L. Huggins, “‘The Most Unlimited Confidence in His Wisdom & Judgement’: Washington as Commander in Chief in the First Years of the French Alliance,” in Lengel, *A Companion to George Washington*.

¹⁵ Piers Mackesy, *The War for America, 1775–1783* (Lincoln: University of Nebraska, 1993), 349.

¹⁶ John A. Nagy, “George Washington, Spymaster,” in Lengel, *A Companion to George Washington*, 349–350.

¹⁷ *Primer*, 26–27.

¹⁸ *Ibid.*, 26.

¹⁹ Kenneth A. Daigler, *Spies, Patriots, and Traitors: American Intelligence in the Revolutionary War* (Washington, DC: Georgetown University Press, 2014), 136–137.

²⁰ “VIII: To John Hancock, 11 September 1777,” *Founders Online*, NARA, available at <<https://founders.archives.gov/documents/Washington/03-11-02-0190-0009>>.

[Original source: *The Papers of George Washington*, Revolutionary War Series, vol. 11, August–October 1777, ed. Philander D. Chase (Charlottesville, VA: University Press of Virginia, 2001) 200–201.]

²¹ Daigler, *Spies, Patriots, and Traitors*, 131, 214.

²² *Ibid.*, 174–177.

²³ *Primer*, 28–29.

²⁴ “Revolutionary War Battles,” George Washington’s Mount Vernon, available at <<https://www.mountvernon.org/george-washington/the-revolutionary-war/washingtons-revolutionary-war-battles/>>.

²⁵ See, for example, Lengel, *General George Washington*, chap. 14.

²⁶ *Ibid.*, 275.

²⁷ *Ibid.*, 275–276.

²⁸ *Ibid.*; Wayne Bodle, *The Valley Forge Winter: Civilians and Soldiers in War* (University Park: Pennsylvania State University Press, 2002), 146–147.

²⁹ See, for example, Paul Lockhart, *The Drillmaster of Valley Forge: The Baron de Steuben and the Making of the American Army* (New York: HarperCollins, 2008).

³⁰ See, for example, chap. 15, “Monmouth,” in Lengel, *General George Washington*.

³¹ Robert Middlekauff, *Washington’s Revolution: The Making of America’s First Leader* (New York: Alfred A. Knopf, 2015), 70–74.

³² *Primer*, 31–32.

³³ “From George Washington to John Augustine Washington, 20 June 1775,” *Founders Online*, NARA, available at <<https://founders.archives.gov/documents/Washington/03-01-02-0009>>. [Original source: *The Papers of George Washington*, Revolutionary War Series, vol. 1, 19–20.]

³⁴ Bruce Chadwick, *The First American Army: The Untold Story of George Washington and the Men Behind America’s First Fight for Freedom* (Naperville, IL: Sourcebooks, Inc., 2005), 227.

³⁵ Bodle, *The Valley Forge Winter*, 132–134.

³⁶ *Ibid.*, 126–130.

³⁷ *Ibid.*

³⁸ *Ibid.*, 165–168.

³⁹ *Ibid.*, 175–177.

⁴⁰ *Ibid.*, 169–171.

⁴¹ Nathaniel Philbrick, *Valiant Ambition: George Washington, Benedict Arnold, and the Fate of the American Revolution* (New York: Viking, 2016), 197.

⁴² Ricardo A. Herrera, “‘Our Army Will Hut This Winter at Valley Forge’: George Washington, Decision Making, and the Councils of War,” *Army History* 117 (Fall 2020), 12.

⁴³ Nathaniel Philbrick, *In the Hurricane’s Eye: The Genius of George Washington and the Victory at Yorktown* (New York: Viking, 2018), 10, 112.

⁴⁴ *Ibid.*, 151, 174–175.

⁴⁵ David Head, *A Crisis of Peace: George Washington, the Newburgh Conspiracy, and the Fate of the American Revolution* (New York: Pegasus Books, 2019), 34–36, 62–63; William M. Fowler, Jr., “‘High Time for Peace’: George Washington and the Close of the American Revolution,” in Lengel, *A Companion to George Washington*, 299; Lengel, *General George Washington*, 349.

⁴⁶ CJCSI 1800.01F, 1.



Cyber crew lead assigned to 800th Cyber Protection Team, Joint Force Headquarters Cyber–Air Force, poses for photo in front of 9th Expeditionary Bomb Squadron B-1B Lancer at Royal Air Force Fairford, United Kingdom, October 8, 2021 (U.S. Air Force/Colin Hollowell)

Cyber Deterrence Is Dead! Long Live “Integrated Deterrence”!

By James Van de Velde

The demands that Congress, some strategists, and many academics make of cyberspace deterrence are unrealistic in the extreme.¹ Many want the Department of Defense (DOD) to

freeze adversary military or influence operations or the theft of American intellectual property (IP) entirely through the simple threat of interfering with adversary computer code, presum-

ably imperiling the function of either adversary military systems or civilian infrastructure. Such strategic thinking is hopelessly naïve because such threats are insufficiently credible to deter malicious cyberspace activities, which generally fall below the level of armed conflict.²

Commanders conduct cyberspace operations³ to “retain freedom of maneuver in cyberspace, accomplish the joint force

Dr. James Van de Velde is a Professor in the Dwight D. Eisenhower School of National Security and Resource Strategy at the National Defense University. He is also an Associate Professor at the National Intelligence University and Adjunct Faculty in the School of Advanced International Studies at Johns Hopkins University.



Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger gives update about U.S. Government's concerns that Russian government may be preparing a cyber attack against U.S. critical infrastructure, during press briefing at the White House, March 21, 2022 (Reuters/Leah Millis)

commander's objective, deny freedom of action to adversaries, and enable other operational activities."⁴ But cyberspace operations are not magic, and neither is deterrence. The retaliatory act (that is, punishment) must be slightly greater than but proportional to the initial act; a disproportional act will trigger retaliation. (DOD, for instance, cannot shut down the Chinese electrical grid or air traffic control because China stole Google's source code, Office of Personnel Management data, some defense technology, or an upcoming iPhone design.)

Cyberspace operations run the gamut from minor interference with Web sites and phishing attacks to accrue information (that is, espionage) to disruption of the functioning of critical infrastructure, such as electrical grids, dams, water purification, election systems, air traffic

control, communication networks, and the like, likely causing mass secondary casualties in many cases.

However, just as with sea or air deterrence, DOD cannot shape all adversary behavior in the cyber domain via cyber deterrence. DOD cannot, for instance, end Russian support for Ukrainian separatists by threatening an air deterrence attack on Russian military sites or cities. The same is true with sea deterrence: it is not credible to expect the threat of punishment from sea platforms alone to change China's threats to Taiwan or its island-creation/sovereignty-expansion campaign. Likewise, it is wrong to expect the threat of punishment via cyberspace alone to stave off Russian hybrid warfare or espionage, nor Chinese influence operations or intellectual property theft. These activities fall below the level of

armed conflict. Some adversary cyberspace activity can be deterred by U.S. cyberspace operations, but some are much harder to deter via threats of punishment through cyberspace.

The United States has generally attempted to deter adversary use of cyberspace to conduct IP theft or influence operations through law enforcement mechanisms (indictments of individual Russian or Chinese cyber actors) or *démarches*. In short, the United States has attempted to discourage malicious adversary cyberspace operations below armed conflict via harsh letters: indictments and diplomatic complaints.

To date, adversaries have not conducted any "cyber Pearl Harbor" events—that is, shutting down/attacking U.S. critical infrastructure or military forces.⁵ First, they have no reason to

do so in peacetime. Such attacks would not serve any purpose in peacetime and would most certainly be met with severe U.S. retaliation, either via cyberspace or through kinetic attack. Second, cyberspace deterrence is relevant at the strategic level and likely does represent a level of credible punishment. Should an adversary state shut down U.S. critical infrastructure, such as a large section of the electrical grid, the United States most likely would shut down that attacking state's electrical grid or other critical infrastructure to demonstrate its strategic deterrent via cyberspace.

In short, the smaller the cyberspace operation (distributed denial of service, IP theft, espionage, or influence operations), the more likely an *asymmetrical* act by the entire U.S. Government would be undertaken to effect punishment. The greater the cyberspace event (disruption of military forces in conflict, strategic cyberspace attack against infrastructure), the more likely a *symmetrical* (cyberspace) operation would be conducted.

Is the Cyber Domain Somehow Different?

Cyberspace competition is occurring every day. The effects that cyber weapons have and can have on infrastructure are quite real: they can make weapons systems fail and critical infrastructure—air traffic control, rail lines, traffic lights, power grids, hydroelectric dams, purification systems, mass media networks, communications networks, financial systems—go dark or be disrupted. Cyber weapons may not easily kill large numbers of people—though mass outages of electrical grids or attacks on airlines might indeed kill hundreds or thousands—but that does not mean their effects are mere nuisances. Their use is a form of armed conflict and can affect a nation's confidence in its weapons systems or communications or its ability to supply troops or feed civilians. Society is so reliant on computer systems that successful disruption of such systems is an immediate disruption of life as we live it.

The United States is also struggling daily with conventional (that is,

noncyber) challenges from China, Russia, Hizballah, Iran, the so-called Islamic State, al Qaeda, the Taliban, and criminal hacking groups. All such challenges have a cyber component. Although cyber is now considered the fifth domain of warfare by DOD (the others being land, sea, air, and space), cyber operations ought not to be viewed as stand-alone military options apart from the other domains.⁶ The United States defends itself in all domains and uses military forces in all domains to defend itself in a manner and combination it chooses. So the cyber domain is not different from the others, though it is much more adversarial in that competitor activity occurs daily in the cyber domain—much more than in the other domains, most especially with activity below the level of armed conflict.

The Fundamentals of Deterrence Do Indeed Apply to Cyberspace

Deterrence is based on denial (protecting against an adversary's attempt to attack) and punishment (inflicting unacceptable costs on the attacker for having conducted an attack). Previously, almost all our cyber deterrence efforts have been defensive. Without both elements—denial and punishment—deterrence will be weak or will fail.⁷

Deterrence via denial alone is ultimately impossible. The victim is always in the miserable position of trying to discern adversary accesses and stop intrusion code written specifically to enter the victim's networks and conduct malicious operations in secret. In short, perfect cyber defense alone is impossible, just as air defense alone would be inadequate to deter all air attack from everywhere.

Deterrence via cost imposition is also hard. Many cyber response operations cause little pain, and the unshakeable U.S. commitment to international law makes it harder for the country to contemplate and conduct operations via cyberspace that might violate the target's sovereignty or that of third parties.

Deterrence cannot be accomplished solely by a robust, threatening public (declaratory) statement. Nuclear deterrence was made credible by the fielding

of multiple nuclear-capable weapons systems, with a robust and redundant command and control network, the integration of nuclear weapons within larger warfare objectives, the creation of a single integrated operational plan for the employment of such nuclear weapons, the stationing of U.S. forces forward in theaters to serve as trip wires, and a strong declaratory statement with explicit and implicit redlines for conflict. The highest levels of the U.S. Government exercise nuclear forces frequently; no one doubts U.S. resolve. Good deterrence requires the demonstration of both defensive and offensive capabilities (such as exercises and technology demonstrations) to send a signal to adversaries.

The differences between nuclear and cyber deterrence, however, are significant. With nuclear deterrence, the United States must deter the single nuclear explosion. With cyber deterrence, the United States is managing an ongoing, constant problem and a spectrum of malicious activity from the small (influence operations) to the strategic (attacks on infrastructure).⁸

In the cyber realm, we cannot simply exercise or demonstrate our capabilities to the world at an airshow or weapons fair, and so we refrain from establishing clearly marked red lines, opting instead to lead by example, by not stealing proprietary information or attacking the critical infrastructure or key resources of another state. Unfortunately, the United States runs the very real risk of trivializing genuine cyberspace attacks, such as the North Korean attack against Sony in November 2014 and the denial-of-service attack against TV5Monde in France in April 2015—not to mention the massive theft of U.S. assets and industrial and intellectual property by China—by calling them “vandalism.”

Norms are created through practices mutually accepted and conducted by states. Such norms became the basis of the Law of the Sea, our conduct in space, and our treatment of warships at sea, and thus emerged as customary international law. Therefore, intrusions directed against us and left unanswered will begin to gain a level of international

acceptance, no matter how many *dé-marches* are issued. Thus, good cyber deterrence policy depends on both international norms promulgated on paper within international forums and clearly executed and well-signaled responses to unacceptable activity.

Successful deterrence is a function of establishing norms, denying benefits, and imposing costs. Each military domain contributes differently to warfare; operating in each domain carries different costs and benefits. If it does not shape the domain, the United States will inevitably end up reacting to norms set by others, good or bad. Whereas most nations tend to respect the traditional rules of peacetime behavior in the land, sea, air, and space domains, many adversaries exploiting cyberspace today ignore the traditional rules of conduct, warfare, and sovereignty.

Detering Kinetic Conflict and Malicious Cyberspace Operations via All Domains

Cyber deterrence means different things to different people. Malicious cyber activity by adversaries does not necessarily have to be deterred by reciprocal cyber activity; it can be deterred by cost imposition effected by operations in the other domains as well as a whole-of-government approach, including sanctions, public attention, diplomacy, and private-sector activity. Similarly, malicious activity by adversaries outside the cyber domain (in the other domains) may be deterred by U.S. cyberspace operations. The United States, therefore, ought to consider use of not only cyberspace capabilities but also kinetic capabilities or other instruments of power to deter malicious cyberspace activity and use of both kinetic and cyberspace capabilities to deter traditional kinetic conflicts.

Cyber deterrence, therefore, should not be delimited as cyber vs. cyber operations but instead—just like all the other domains—should be placed into a larger deterrence model that involves all military domains, as well as the diplomatic, law enforcement, and economic arms of the U.S. Government. Cyber operations also

can contribute to larger strategic (kinetic) deterrence, given that cyber is the lifeblood for all domains. Being able to use cyber capabilities in the land, air, sea, and space domains to deter adversary behavior in those domains is vital. In short, the United States must use cyberspace operations to deter both malicious adversary cyberspace activities and kinetic conflict. Thus, a better phrase to understand deterrence and cyberspace may be *deterrence through cyberspace*.

Academic publications use the term *cross-domain deterrence* to describe what happens when a capability in one domain constrains adversary behavior in another through the denial of benefits or the imposition of costs on the adversary's selected course of action.⁹ A deterrence strategy that uses the capabilities of the full span of diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL) instruments of national power will shape perceptions and actions of both existing and would-be adversaries across domains and will yield a more robust deterrence strategy.

Deterrence and Escalation

By definition, punishment for a malicious event must outweigh the value of the malicious event or the attacker will continue initiating such events. Deterrence fails if unacceptable damage is not feared by the attacker. By definition, therefore, deterrence based on punishment is escalatory. Thus, on the one hand, the United States must plan to inflict escalatory damage on a potential attacker to effect deterrence. On the other hand, the Nation cannot threaten exceptional damage for minor adversary cyberspace operations that merely create small effects or accrue small amounts of data or IP. This is true for all the domains: small violations of sea or air space cannot be deterred via the threat of massive kinetic or cyberspace damage. An exceptionally disproportional response would trigger, not control, escalation and thus is not credible.

To address this reality, DOD has begun a maneuver strategy of persistent engagement: the continuous execution of

the full spectrum of cyberspace operations to contest adversary campaigns and objectives. Persistent engagement means that DOD is going to press adversaries' cyberspace plans and objectives—thwarting attempts to conduct IP theft or influence operations or emplace capabilities on U.S. critical infrastructure by constantly being in the face of its cyber adversaries. Creating such friction in cyberspace will bring about a level of deterrence by demonstrating to cyber adversaries that there is a cost to their malicious activity. Until the strategy was implemented, the United States had not inflicted any punishment, friction, or resistance of any significant kind for activities below armed conflict. (Why should cyber adversaries cease malicious activity, which was accruing much benefit at no cost?) Thus, the friction today stems from the long-term and gradual introduction of a level of deterrence through cyberspace; persistent engagement is the operational implementation of cyber deterrence.

Cyberspace effects will never equal the effects of a nuclear weapon or mass kinetic attack. Thus, the risk of escalation from cyberspace effects to nuclear war is small. So far, cyberspace effects have not provoked much, if any, escalation. Regrettably, the fear of escalation has wrongly colored many perceptions; many policymakers and academics fear cyberspace operations, thinking any such operation will be met with escalation to the kinetic stage of conflict. This is both counterintuitive and historically not true.

Integrated Deterrence

In a speech to U.S. Indo-Pacific Command on April 30, 2021, Secretary of Defense Lloyd Austin stated:

[O]ur challenge is to ensure that our deterrence holds strong for the long haul, across all realms of potential conflict. . . . We'll use existing capabilities, and build new ones, and use all of them in new and networked ways—hand in hand with our allies and partners. Deterrence . . . now spans multiple realms, all of which must be mastered to ensure our security in the 21st century. And deterrence now demands far more coordination, innovation, and cooperation

from us all. Under this integrated deterrence, the U.S. military isn't meant to stand apart, but to buttress U.S. diplomacy and advance a foreign policy that employs all instruments of our national power.

What we need is the right mix of technology, operational concepts, and capabilities—all woven together in a networked way that is so credible, flexible, and formidable that it will give any adversary pause. We need to create advantages for us and dilemmas for them. That kind of truly integrated deterrence means using some of our current capabilities differently. It means developing new operational concepts for things we already have. And it means investing in quantum computing and other cutting-edge capabilities for the future, in all domains.¹⁰

Deterrence today, according to Secretary Austin, leverages all instruments of national power (DIMEFIL), advances cross-domain deterrence across all commands, and incorporates emerging technologies, such as quantum computing and artificial intelligence, to provide decision advantage.

Integrated deterrence is intended to expand the nuclear deterrence paradigm and comprises deterrence regimes across all domains and across the spectrum of competition by leveraging all instruments of national power, dominating the information space, and advancing cross-domain deterrence across all combatant commands. It will involve allies and partners and harness emerging technologies and concepts. Integrated deterrence presumably demands a more tailored approach to deterrence, specific to adversaries and scenarios and addressing specific political circumstances. It is intended to support and be aligned with other U.S. national security capabilities and to leverage the support of allies and partners.

By themselves, cyberspace operations are unlikely to shift adversary behavior in high-end armed conflict, where states are committing lots of kinetic conflict. And they are unlikely to restore deterrence in situations where an adversary can dominate in conflict (where the adversary has regional conventional supremacy over a

Figure 1. Continuum of Competition to Conflict

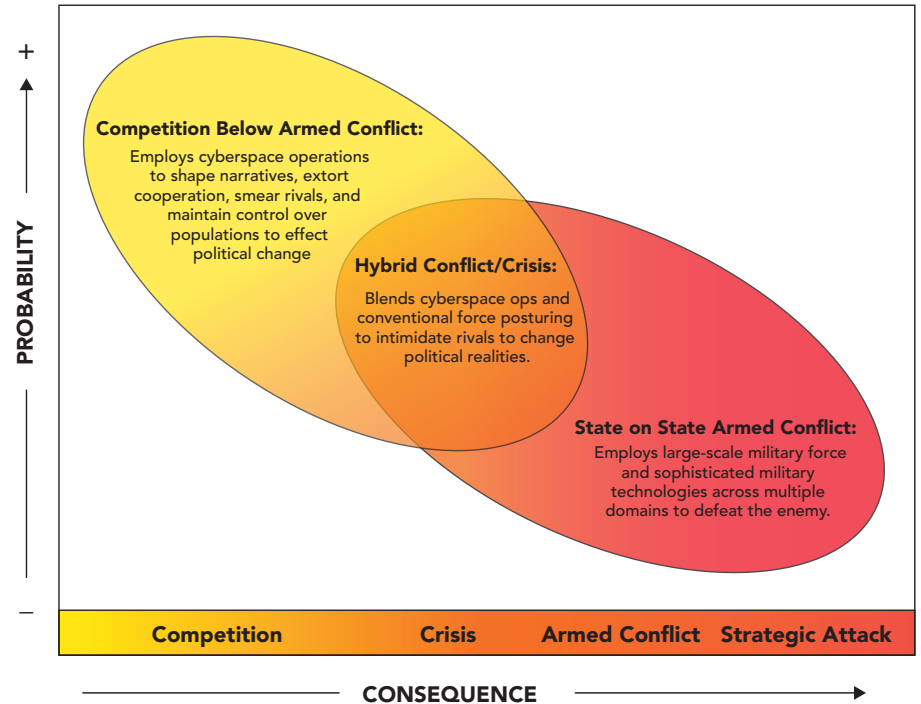
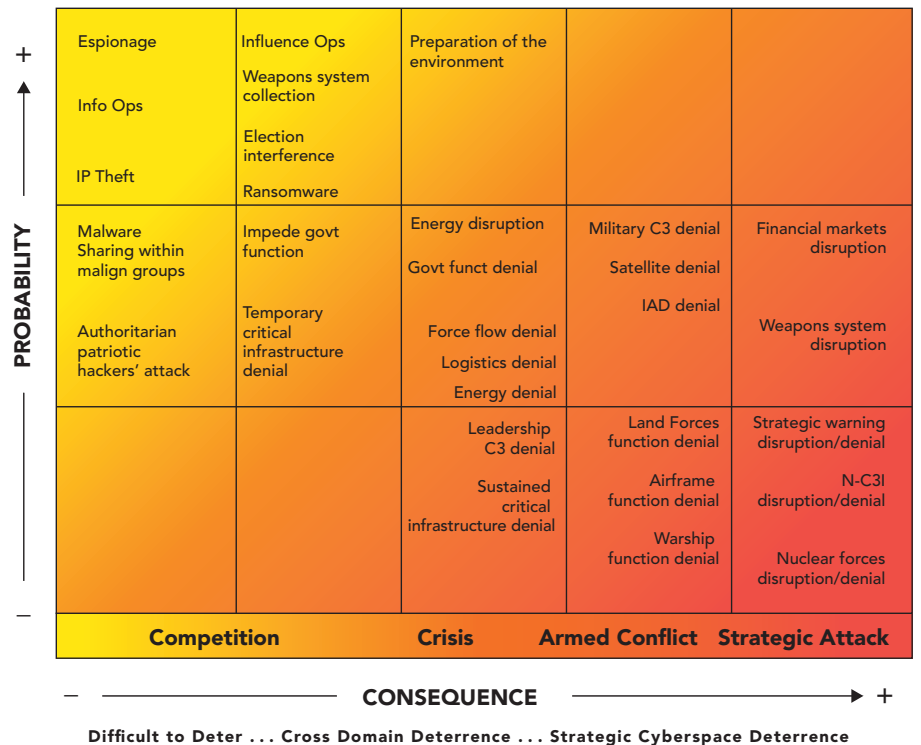


Figure 2. Cyberspace Operations Across the Continuum





Exercise support staff launch scenario injects for training scenario as part of exercise Tacet Venari, held at U.S. Air Forces in Europe Regional Training Center, Ramstein Air Base, Germany, March 8, 2019 (U.S. Air Force/Renae Pittman)

EXIT



WHITE CELL





25D cyber network defender with Pennsylvania National Guard works network defense during Cyber Shield 20, at Fort Indiantown Gap, Pennsylvania, September 20, 2020 (Pennsylvania National Guard/Angela King-Sweigart)

specific situation) or where an adversary has a much greater political stake. But because they historically have not elicited escalation in the stage of competition, cyberspace operations may be uniquely appropriate to signal stake and deter armed conflict in a crisis.

Using Cyber to Effect Deterrence Within a Crisis

Conducting cyberspace effects to impose costs on an adversary in a confrontation might have a potent impact on the adversary if employed in the early stages of the unfolding crisis. Changing the adversary's cost proposition might provide an escalation control means. And beyond pure cost imposition, introducing uncertainty in the decisionmaking of an adversary—by showing a capability and willingness to act—can provide a significant deterrent.

Cyberspace effects are likely most potent if employed during the early stages of an escalating conflict, before actual kinetic conflict commences. Developing a range of kinetic and cyber capabilities affords commanders multiple options to be employed to deter an adversary while showing U.S. resolve to reduce escalation.

Cyber effects, which are reversible and do not directly destroy infrastructure or cause loss of life, may be considered less escalatory than other options available within DOD because the absence of physical devastation or loss of life provides a face-saving off-ramp to an adversary. An adversary that recognizes a likely U.S. cyber effect on its networks but suffers no loss of life may be more inclined to de-escalate from a crisis. Alternatively, a kinetic (and public) response may corner the adversary and force a reply.

Similarly, because cyberspace operations are nonkinetic and reversible, they may represent small moves up an escalation ladder and signal less stake than kinetic options. Choosing the most appropriate operation in mid-crisis, to effect intra-crisis deterrence, falls to the Commander in Chief. Having nonkinetic options at least allows the Commander in Chief to signal a degree of U.S. stake in a crisis, when perhaps the adversary might assume the United States had none.

Most cyberspace operations will, therefore, likely occur early in any escalation, will have their most important deterrent effects in the crisis phase (before armed conflict), and will likely diminish quickly as the sides tighten cyberspace defenses and defeat subsequent attempts to produce effects. They will likely lose effectiveness in the armed conflict phase, as physical infrastructure is destroyed

and network defensive measures are employed. Cyberspace operations targeted at adversary weapons systems are more appropriate for the armed conflict phase but are of little use in the crisis phase to deter or message (signal) an adversary.

Cyberspace capabilities can be either transparent or nontransparent. Transparent capabilities can deter an adversary by exposing U.S. access and capabilities purposefully, to reveal an adversary's network vulnerabilities and create a loss of confidence. Nontransparent capabilities can hold an adversary at risk of preemption and support escalation control, if needed.

Additionally, the ambiguity of attribution associated with nontransparent cyber effects can further limit the chances of escalation and kinetic retaliation.

Effects employed discreetly that cannot be directly and definitively attributed to the United States provide a layer of uncertainty as to who was responsible for creating the effect. This in turn may cause an adversary to hesitate to launch a retaliatory or escalatory response. Thus, cyberspace operations can target non-warfighting targets prior to any conflict to demonstrate stake in an issue and signal U.S. resolve, creating a pause in the planning and conduct of adversary military operations.

Cyberspace operations are especially well suited to be introduced asymmetrically to introduce unpredictability—another tenet of deterrence—in a crisis or confrontation. Such operations signal a willingness to become involved in an issue and to expose unanticipated adversary vulnerabilities while not causing significant physical damage. The message to the adversary is to stop before events escalate to kinetic conflict, before additional costs are inflicted, and before face-saving off-ramps are excluded. Cyberspace operations, therefore, may offer the best means to avoid large-scale conflict.

Thus, cyberspace operations may contribute to preventing armed conflict if employed early in a crisis or conflict by shutting down certain adversary weapons systems or interfering with certain high-value civilian (counter-value) targets, such as infrastructure, social

media, or institutions of significant value to a nation, thus sowing surprise and doubt in the mind of the adversary. Such operations may therefore contribute to escalation control in all the domains (cross-domain deterrence).

A portion of the U.S. Cyber Mission Force (CMF) should focus away from symmetric cyber-on-cyber and counterforce options and toward a strategic deterrence and escalation control mission. This shift would rebalance the CMF toward offering strategically powerful effects in support of global and regional strategic deterrence and escalation control. Rebalancing is critical to ensure that the CMF is postured to offer effects through all phases of conflict: to deter adversary aggression, control escalation, and prevail in conflict if deterrence fails. Adversary targets must be carefully selected to control escalation while not encouraging horizontal or vertical escalation.

Prerequisites for Strong Deterrence Through Cyberspace

Providing the warfighter with strong and reliable networks will enable successful operations. Such preparation creates a deterrent effect by demonstrating that military operations will continue unimpaired by potential adversaries' actions in cyberspace. Adversaries must believe that when they act in cyberspace against U.S. interests, they risk undesirable endstates. Conversely, if potential adversaries perceive that U.S. forces are unable to conduct assigned missions due to shortcomings in cyber capabilities, they will be emboldened to continue cyberspace operations against DOD networks.

Because cyberspace is the lifeblood for all domains, it cannot be a source of vulnerability to DOD operations. Hardened networks that effectively resist attack and exploitation can impose greater costs on would-be adversaries. Resilient networks, designed to operate in degraded states, are prerequisites for deterrence and will promote the idea of futility in the mind of potential adversaries.

There can be no deterrence if adversaries perceive their activities as

invulnerable to detection and thus act without fear of consequence. The accurate and timely identification of hostile actors is critical, therefore, to holding adversaries responsible for their actions or intentions. If an adversary knows that DOD can correctly and quickly attribute actions in cyberspace, then the adversary will immediately be concerned. Attribution capabilities are, therefore, paramount for strong deterrence. Enhanced research and development are needed to improve intelligence and criminal investigation capabilities.

Once attribution is determined, DOD must have appropriate policies and authorities to prevent or, if needed, respond to hostile acts in cyberspace. Would-be adversaries can be deterred if DOD authorities provide a rapid, unified response to protect the Nation.

To enhance domestic cyber defense, DOD must continue to develop and lead international partnerships for collective defense. International coalitions can provide DOD additional capabilities to detect malicious cyber activity and can hamper actors from establishing safe havens in geographic areas of partner nations. Additionally, the United States should incentivize all friendly foreign governments to address malicious cyber activity originating within their borders.

Cyber capabilities are rapidly evolving. For DOD to remain a key player in cyberspace, not only is adoption of new and emerging technologies essential, but also development of new capabilities is required to bolster DOD prowess, effectively adding to greater deterrent effect.

Increasingly, components are developed first for commercial applications, then adopted for weapons systems. Global supply chains and research and development processes create and distribute technologies—with the associated danger that a malign actor might seek to divert or influence the supply chain for strategic purposes. Strategies must be developed to counter the corruption of DOD supply chain networks.

Showcasing DOD capabilities and fortitude in cyberspace is vital. DOD prowess to detect, defend against, and respond to hostile acts must be well known,

or there can be no deterrence. Capability demonstrations and military exercises are common shows of force in the physical domain; analogous displays should be appropriately employed in the cyber domain wherever and however possible.

U.S. Cyber Command likely needs more teams. Ample forces will afford the United States opportunities, options, cross-education, capability sharing, access, credibility, and greater historical knowledge and experience. The goal for deterrence through cyberspace is the absence of conflict, of course. Good deterrence through cyberspace includes discerning and offering off-ramps for adversaries to avoid escalation. Thus, DOD ought to examine the best use of cyber forces: to target them against adversary military systems for use in conflict (which may never occur) or to use them persistently below the level of armed conflict to create friction and frustrate adversary efforts at influence operations, IP theft, election interference, and overall information operations. What is the better use—or balance—within our cyber teams for these competing missions?

Conclusion

Cyberspace operations offer the President options alongside other elements of national power for the purposes of deterring adversary actions. Like all domains, the cyber domain cannot win or lose a conflict or control a crisis alone. Like all domains, it can complement other instruments of U.S. power and assist the warfighter facing military targets during conflict. But the cyber domain may have especially potent cross-domain effects as well as crisis control capabilities that the other domains cannot offer. Fortunately, cyber effects tend not to be escalatory—a positive element for crisis planning involving cyberspace options.

All military domains afford levels of deterrence at the strategic level but struggle to effect deterrence below the level of armed conflict. The cyber domain is no different. Deterrence in cyberspace is best effected through continuous engagement with malicious actors, who use cyberspace to despoil

international norms. Only through such persistent engagement will any level of deterrence be realized. JFQ

Notes

¹The U.S. Cyberspace Solarium Commission, for instance, in its March 11, 2020, final report, proposes a strategy of “layered cyber deterrence.” See “Our Report,” U.S. Cyberspace Solarium Commission, available at <<https://www.solarium.gov/>>. According to Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as Amended Through February 15, 2016), 67, *deterrence* is the “prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits.” *Cyberspace* is defined as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,” JP 1-02, 58.

²See Michael P. Fischerkeller and Richard J. Harknett, “Deterrence Is Not a Credible Strategy for Cyberspace,” *Orbis* 61, no. 3 (Summer 2017), 381–393; Timothy M. McKenzie, *Is Cyber Deterrence Possible? Perspectives on Cyber Power*, CPP-4 (Maxwell AFB, AL: Air University Press, 2017), available at <https://media.defense.gov/2017/nov/20/2001846608/-1/-1/0/cpp_0004_mckenzie_cyber_deterrence.pdf>.

³*Cyberspace operations* are defined as the “employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace,” JP 1-02, 58.

⁴JP 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), ix, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf>.

⁵Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, identifies 16 critical infrastructure sectors of key importance to the U.S. Government: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

⁶The Department of Defense (DOD) does not use the term *cyber warfare* because *warfare* is a policy condition decided by the President and Congress. An unofficial DOD definition

of cyber warfare can be found in “Joint Terminology for Cyberspace Operations,” Office of the Vice Chair of the Joint Staff, 16, available at <<https://info.publicintelligence.net/DoD-JointCyberTerms.pdf>>: “Armed conflict conducted in whole or in part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions.” (Not all cyber attack is cyber warfare, but all cyber warfare is armed conflict.)

⁷See *Deterrence Operations, Joint Operating Concept*, vers. 2.0 (Washington, DC: DOD, December 2006), available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337>.

⁸For concept of competition, see Air Force Doctrine Publication 3-05, *Special Operations* (Washington, DC: Headquarters Department of the Air Force, February 1, 2020), available at <https://www.dctrine.af.mil/portals/61/documents/afdp_3-05/3-05-afdp-special-operations.pdf>. Specifically, regarding the competition continuum, see *Special Operations Forces Within the Competition Continuum* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, 2020), available at <http://www.dctrine.af.mil/Portals/61/documents/AFDP_3-05/3-05-D03-SOF-Competition-Continuum.pdf>.

⁹See Celeste A. Drewien, “Cross-Domain Deterrence” (presentation at U.S. Air Force Academy, Colorado Springs, CO, April 26, 2019), available at <<https://www.osti.gov/servlets/purl/1644932>>; King Mallory, *New Challenges in Cross-Domain Deterrence* (Santa Monica, CA: RAND, 2018), available at <<https://www.rand.org/pubs/perspectives/PE259.html>>; Jon R. Lindsay and Erik Gartzke, ed. *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019); Vincent Manzo, *Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?* INSS Strategic Forum No. 272 (Washington, DC: NDU Press, December 2011), available at <<https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf>>; Tim Sweijs and Samuel S. Zilincik, “The Essence of Cross-Domain Deterrence,” in *NL ARMS Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijs (The Hague: T.M.C. Asser Press, 2020), available at <https://doi.org/10.1007/978-94-6265-419-8_8>.

¹⁰Lloyd Austin, “Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command,” April 30, 2021, Camp H.M. Smith, HI, available at <<https://www.defense.gov/news/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/>>.

Four Army CH-47F Chinook helicopters from 1st Battalion, 214th Aviation Regiment (General Support Aviation Battalion), 12th Combat Aviation Brigade, prepare to land during exercise Falcon Autumn 22 at Vredepeel, Netherlands, November 4, 2022 (U.S. Army/Thomas Mort)



A Mission Assurance Assessment of Threats to Missions and Force Protection Planning

By Michael J. Borders, Jr., and Miller Carbaugh

After the Cold War, the United States enjoyed such an uncontested or dominant superiority in every domain that the Department of Defense (DOD) could deploy forces when it wanted, assemble them

where it wanted, and operate them as it wanted. Perhaps because of this history, combined with the objectives in the 2018 National Defense Strategy (NDS), DOD components have focused on the development of new

offensive and lethal capabilities and concepts with the unstated assumption that, once developed, these capabilities would be available. The following scenario describes how these assumptions can adversely affect DOD force projection capabilities.

A crisis occurs, a combatant commander is assigned to respond by using a specific operations plan or developing

Colonel Michael J. Borders, Jr., is the Commander of Detachment 3, Air Force Installation and Mission Support Center, Hurlburt Field, Florida. Miller Carbaugh is a People Operations Generalist at the Heritage Foundation.



Soldier assigned to Force Protection Platoon, 3rd Battalion, 66th Armored Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division, maintains perimeter security from top of Humvee during gate runner exercise conducted at Camp Herkus, Lithuania, April 13, 2022 (U.S. Army National Guard/Agustín Montañez)

a contingency plan, and forces begin to flow. However, what if the forces that enable either of these plans are delayed or reduced, or they do not show up at all? Claiming that this could never happen or that we would “figure it out” is not sufficient. There is a serious need for a better response. If, at all levels of command, these forces are delayed, degraded, or completely unable to function as needed, then the joint force commander’s decision space is reduced, adversely affecting the decisionmaking process and ultimately risking mission failure.

The Current Security Environment

The unclassified 2018 summary of the NDS states that “the homeland is no longer a sanctuary” and notes that the United States faces, among other challenges, a “reemergence of long-term strategic competition.” Strategic competition in this environment “requires

the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military.”¹

The security environment is described here as one in which terrorism remains a persistent condition, transnational criminal organizations and other malicious nonstate actors have increasingly sophisticated capabilities, and revisionist powers and rogue regimes will use ambiguous or denied proxy operations to achieve their ends short of open warfare.² Adversaries have enjoyed the opportunity to identify and categorize critical capabilities and associated vulnerabilities of the joint force; their resulting strategies could create confusion, disrupt or delay force projection, and divert military resources in the transition to war.

Great Powers and rogue regimes have been able to conduct a campaign of operational preparation of the environment (OPE) nearly autonomously

both inside and outside the continental United States (OCONUS). Current U.S. protection efforts do not align with the threats outlined in the NDS and endanger DOD’s ability to flow forces from the homeland to OCONUS combatant commanders, increasing the risks associated with projecting military power. Adversaries are improving their existing capabilities and seeking new, asymmetric means to delay, disrupt, and cripple our force projection, warfighting, and sustainment capabilities by targeting military and civilian infrastructures—within the homeland and abroad—that our military forces depend on.

Campaigns Against Critical Infrastructure

The building blocks that DOD needs to conduct successful military campaigns in the Great Power era are predominantly located on its installations and bases across the homeland. These

building blocks are reliant on critical infrastructure located both inside and outside the boundaries of DOD authorities and control. Key questions to consider are:

- How do commanders ensure they can project forces forward when projection relies on critical infrastructure outside their authority and is exposed/targeted for nontraditional attacks?
- What are the nicks and cuts our adversaries can inflict on this critical infrastructure that commanders must account for, and how can they work to mitigate these?

Regarding these questions, specifically concerning China and Russia, the Office of the Director of National Intelligence warns:

China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States. . . .

Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.³

Recent Targeting Activities by Adversaries

Adversaries are conducting OPE and actively targeting U.S. critical infrastructure through hybrid and blended operations that take advantage of legal restrictions and friction points between U.S. departments and agencies. Their overarching goal is to hold our centers of gravity at risk and impact force projection; they are capable also of sowing discontent during steady-state activities and therefore of ultimately destabilizing and delegitimizing our government. Their near-term goals are simply to identify and categorize

attack vectors in the event of a larger conflict. Examples over the past few years include:

- Software engineer Xudong “William” Yao was wanted for theft of proprietary information, including nine copies of control system source code and systems specifications from a Chicago locomotive manufacturer in 2019. He remains at large and is suspected of having returned to China.⁴
- More than two dozen U.S. universities were targeted by Chinese hackers in 2019 as part of an effort to steal military maritime technology research.⁵
- In 2020, there was an attempt to disrupt the power grid by drone, when a DJI Mavic 2 approached a Pennsylvania power substation with intent to “disrupt operations by creating a short circuit.”⁶ This was the first known instance of a modified, uncrewed aircraft system being used to specifically target U.S. energy infrastructure.⁷
- Russian state-sponsored advanced persistent threat actors targeted state, local, tribal, and territorial governments, and aviation networks in 2020, successfully compromising networks and exfiltrating data from multiple victims.⁸
- In 2019, the U.S. Cybersecurity and Infrastructure Security Agency warned of the possible cyber-espionage threat that Chinese-made drones could pose to U.S. businesses and other organizations that use them.⁹ The notice added that those most at risk were using the aircraft for tasks related to national security or critical infrastructure.¹⁰
- Zhao Qianli, student tourist in Florida, accessed and photographed U.S. Naval Air Station Key West, Joint Interagency Task Force South; he was detained through close base police—local police cooperation and was sentenced to prison, in 2019, for illegal photography of the air station.¹¹
- A National Security Agency senior official warned about rising Chinese hacking against United States in

2018, noting that the hackers were targeting critical infrastructure in possible attempts to lay the groundwork for future disruptive attacks.¹²

- According to a 2019 report by Vietnam Veterans of America, Russian information operations are increasingly targeting troops, veterans, and their families, connecting with prominent members to shape Federal policy with the goals of perpetrating financial fraud, spreading anti-American propaganda, manipulating online public spaces, and sowing discord by exploiting and inflaming national divisions.¹³
- Russian aluminum giant Rusal, previously sanctioned by the United States, purchased a 40 percent stake in an Ashland, Kentucky, plant in 2019. The Kremlin-linked firm invested millions of dollars, raising both economic and national security concerns.¹⁴
- In 2018, intelligence analysts warned that Russian hackers probing the U.S. power grid were achieving many goals through persistent probing; the full extent of their access is largely unknown.¹⁵
- A Justice Department official warned in 2020 that homegrown violent extremists could potentially weaponize the COVID-19 virus and use it against the populace.¹⁶

As these examples demonstrate, gray zone warfare is being conducted both inside and outside the wire in cyberspace. Adversaries will operate in any domain where they perceive they can gain an advantage. Their ongoing OPE requires them to be patient and imaginative and to stay in it for the long haul.

Nonlinear and Nontraditional Way Forward

To ensure force projection from the homeland, DOD must focus sufficient attention on protecting competitor and adversary activities in the steady state short of war (gray zone threats) to protest adversary activities in the transition to war. This distinction is perhaps useful for discussion purposes, but the transition between the two conditions, in

Marine Corps AV-8B Harrier attached to 22nd Marine Expeditionary Unit flies past Navy Aviation Boatswain's Mate (Handler) 1st Class Tu N. Chau during flight operations aboard USS *Kearsarge* in Baltic Sea, August 24, 2022 (U.S. Navy/Taylor Parker)



reality, might not be clear until after it has occurred. Implicit in this limited examination is an assumption that war plan development and review fully consider the spectrum of adversary capabilities.

Through a rigorous assessment of the range of competitors and potential adversaries, their anticipated operational concepts, and their technological tools, DOD must anticipate military problems of future conflict and develop its own operational concepts, both offensive and defensive, to ensure that the joint force can react, deploy, survive, operate, maneuver, and regenerate. Essentially, if the United States wants to deploy forces from a contested homeland in the future, it must think differently about how, where, and with whom it protects those forces in the homeland, starting now. The following represent discussion points and recommended ways to move the conversation forward.

Analyze Competitors, Adversaries, and Capabilities. The need to defend against terrorism is not going away. A new normal exists, with an ever-present, evolving global terrorist threat. However, DOD has a wider range of competitors, potential adversaries, and natural and manmade hazards to consider. Terrorists, insurgents, and those who present the greatest risk to the Nation must not be the only priority; the COVID-19 pandemic serves as an excellent real-life example of a biological hazard's disruption of military operations. A logical first step in planning is to analyze what capabilities DOD may have to counter, now and in the future. This will, of course, have to be a continuous process of identification, evaluation, and red-teaming or wargaming that fleshes out actual threat and hazard capabilities, potential consequences, and useful countermeasures to drive adaptation at the

speed of relevance. This wargaming will have to assume an effective coordinated first punch—with an indeterminable amount of ambiguity following.

The challenge during steady-state operations is that even potential adversaries who pose the greatest risk can minimize their exposure by pretending to be what they are not, through denied or proxy operations and the exploitation of commercially available technology. Therefore, assessing capabilities and creative employment potential is likely a more useful start than trying to identify specific potential adversary or competitor users in advance.

Superior capabilities of the Great Powers and rogue regimes are most dangerous; they require additional analysis of where, when, how, and why they might be used. Such actors may use them in gray zone activities, during the transition to war, and/or during conflict. Although these capabilities are probably already



captured through an existing intelligence requirement, their potential impact on future force protection needs must be the focus of analysis. This analysis must adjust as necessary.

Analyze DOD, Interagency, Allied, and International Partner Capabilities.

Addressing existing challenges requires an assessment of available tools and resources for use in the present. Numerous programs and processes exist to protect DOD personnel, resources, assets, systems, facilities, and information, though they are not currently optimized for the changing security environment. These programs and processes include but are not limited to antiterrorism; law enforcement; physical, information, industrial, personnel, operations, and cyber security; and counterintelligence. Additionally, given the potential of biological threats, force health protection must be part of this analysis. For the near term, a

sufficient assessment of the existing capabilities and capacities of these programs and processes will inform an analysis of potential gaps to follow.

Any such assessment would be incomplete without considering partnerships with interagency and international partners. Numerous Federal agencies, state and local authorities, allies, and other international partners, each with its own source and limit of authority, have capabilities relevant to protecting the joint force. A complete characterization of all these entities is unnecessary at the macro level, though protection planning at each successive level of command must adequately engage the relevant partner organizations in the area. Also, an important consideration in this process is the impact of the security environment on the existing mission and ability of each of these entities to protect relevant populations and infrastructure. Because they

all must cope with finite resources and expanding challenges, identifying efficient and effective means of mutual support will be an ongoing effort.

Identify and Prioritize Gaps and Excesses. With the NDS defining the strategic endstate, the analysis of current and projected adversary capabilities and DOD and partner capabilities defines the starting point. Capability and/or capacity mismatches indicate potential gaps and excesses to prioritize and address. Because any initial analysis will become obsolete quickly in a rapidly changing environment, an iterative process will be necessary to identify new conditions, their influence on existing capabilities, capacities, and excesses, and any changes to gap-solution priorities. Such an effort will require the participation of and coordination among U.S. departments and agencies.

Develop and Implement Solutions. The existing DOD process to identify

potential solutions in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy is a valid approach. To anticipate, analyze, decide, and develop countermeasures at the speed of relevance will likely require new processes that produce some results sooner, which are preferable to comprehensive results that come too late. Speed of action has inherent risk, but the production of faster results is worth this risk.

To ensure DOD employs effective deterrent effects against near-peer aggression, it should develop a special operations forces hybrid warfare capacity focusing on U.S. critical infrastructure. It should determine vulnerabilities and recommend ways to harden U.S. critical infrastructure against exploitable vectors, and build an offensive capability to exploit similar vulnerabilities in revisionist nations. To confidently project power in the gray zone, the U.S. Government must secure our domestic power projection platforms to deny reciprocal strategies from our strategic competitors.

Focus on the Installation Level.

Commanders must now distill the previous four discussion points into an applicable approach at the local level. There must be a recognition that OPE campaigns are ongoing and focused on the U.S. critical infrastructure that enables force projection. Recognizing the analysis and thorough mission decomposition of the specific forces projected forward is key. Successful force projection will likely rely on U.S. critical infrastructure both on and off DOD installations. This process will require a ruthless determination of what is important and how to defend it. The shift in adversary tactics will require installation commanders to develop and implement a more synergized and integrated approach, with intelligence, cyberspace, security, local law enforcement, and other efforts all playing their part to protect the reliant critical infrastructure wherever necessary.

Conclusion

The NDS identifies persistent and rising threats to the homeland, but current legal considerations, especially restrictions, are a challenge. Adversaries continue to conduct OPE in the

near term and take advantage of friction points within the U.S. Government. To protect the homeland, new methods, authorities, and partnerships are required. However, mission owners must start with a prioritization of what enables their mission that extends beyond the wire so that they may be better prepared to answer if forces are delayed, reduced, or unable to show up when a crisis occurs.

DOD leaders will need to rethink how they will execute missions—not only the initial deployments or dispersals but also all activities leading up to the execution order. DOD needs to incorporate real resilience, as well as physical and cyberspace protection, in all its capabilities—supply chain, mission operations, personnel management, and command and control. As expressed in the discussion and recommendations, DOD needs the support of the whole of government, and in many instances the whole of society, to enable it to execute its missions with minimal delays and disruptions. To fail to provide such support will be playing into our adversaries' hands, and history will repeat itself—perhaps with much more devastating consequences. JFQ

Notes

¹ *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), available at <<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>>.

² Ibid.

³ *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), available at <<https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>>.

⁴ "Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China," Department of Justice, July 11, 2019, available at <<https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china>>.

⁵ Dustin Volz, "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets," *Wall Street Journal*, March 5, 2019.

⁶ Brian Barrett, "A Drone Tried to Disrupt the Power Grid. It Won't Be the Last," *Wired*, November 5, 2021, available at <<https://www.wired.com/story/drone-attack-power-substation-threat/>>.

⁷ Ibid.

⁸ *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure* (Washington, DC: Cybersecurity and Infrastructure Security Agency [CISA], January 11, 2022), available at <<https://www.cisa.gov/uscert/ncas/alerts/aa22-011a>>; "Unmanned Aircraft Systems (UAS)—Critical Infrastructure," CISA, February 15, 2017, available at <<https://www.cisa.gov/unmanned-aircraft-systems>>.

⁹ "U.S. Warns of Threat from Chinese Drone Companies," BBC News, May 21, 2019, available at <<https://www.bbc.com/news/technology-48352271>>.

¹⁰ "Unmanned Aircraft Systems (UAS)."

¹¹ "Chinese National Sentenced to Prison for Illegal Photography of U.S. Naval Installation in Key West, Florida," Department of Justice, 2019, available at <<https://www.justice.gov/usao-sdfl/pr/chinese-national-sentenced-prison-illegal-photography-us-naval-installation-key-west>>.

¹² Jim Finkle and Christopher Bing, "China's Hacking Against U.S. on the Rise: U.S. Intelligence Official," Reuters, December 11, 2018, available at <<https://www.reuters.com/article/us-usa-cyber-china/chinas-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OAI1TB>>.

¹³ Kristofer Goldsmith, *An Investigation Into Foreign Entities Who Are Targeting Servicemembers and Veterans Online* (Silver Spring, MD: Vietnam Veterans of America, 2019), available at <<https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf>>.

¹⁴ Simon Shuster and Vera Bergengruen, "A Kremlin-Linked Firm Invested Millions in Kentucky. Were They After More Than Money?" *Time*, August 13, 2019, available at <<https://time.com/5651345/rusal-investment-braidy-kentucky/>>.

¹⁵ Lily Hay Newman, "Russian Hackers Haven't Stopped Probing the U.S. Power Grid," *Wired*, November 28, 2018.

¹⁶ Betsy Woodruff Swan, "How the Coronavirus Is Reshaping Terrorists' Attack Plans," *Politico*, March 27, 2020, available at <<https://www.politico.com/news/2020/03/27/coronavirus-terrorism-justice-department-150870>>.



Napoleon Bonaparte, French painting probably based on 1798 engraving by Elisabeth Herhan and Franz Gabriel Fiesinger, after drawing by Jean Urbain Guérin, oil on wood (Metropolitan Museum of Art)

Napoleon Revisited

By George DiMichele

Since Napoleon Bonaparte's death, in 1821, he has continued to command the fervent interest of many admirers. Military thinkers persist in the search for the secrets of his success. Countless books and articles have been written in an attempt to unlock his astonishing abilities.

The United States would greatly benefit by uncovering such secrets. Great Power competition is on the horizon, national defense costs continue rising rapidly, and national security remains a pressing concern. U.S. leaders need to reexamine Napoleon's methods to see what they can learn from this renowned

military leader to help surmount today's challenges. This article explores Napoleon's military talents, examines his pioneering use of operational art and design, and then argues that the United States must become the 21st-century master of art and design.

Napoleon lived during a transitional period in European history. In the late 18th century, the practice of limited warfare was coming to an end. The French Revolution created upheaval.

Lieutenant Colonel George DiMichele, USAF (Ret.), was an Intelligence Officer in the 445th Airlift Wing, Fourth Air Force, Air Force Reserve Command, at Wright-Patterson Air Force Base, Ohio.

Much larger armed forces took shape; the French *levée en masse* army shook the foundations of military thinking.¹ As a general, Napoleon led the French army to success in Italy in the 1790s, building his reputation as a skillful military leader.² Born in 1769, Napoleon was remarkably young when he engineered those victories, but the experiences were central to transforming General Bonaparte into the great Emperor Napoleon.

An astute student of military history during his youth, Napoleon showed the effect of his education in the way he planned and commanded his conquests.³ Later in life, after fighting many battles, Napoleon claimed that he had gained no new knowledge beyond what he gleaned in his younger years.⁴ This view is surprising, given that in later years he could look back on stunning victories at Austerlitz and Jena, upon which his reputation was built.

Napoleon's battlefield triumphs provide rich examples of his skills and use of speed, maneuver, and surprise. They also point to a conventional, rather than a revolutionary, thinker.⁵ Whereas admirers called him a genius, the facts speak of

something different: it is highly likely his talents were mostly the result of conventional hard work.

Consider his swiftness in battle. He often attacked opponents before their armies could mass in overwhelming numbers.⁶ In 1806, he attacked and defeated Prussia at the battle of Jena-Auerstedt before Prussia's allies could join. During the climactic battle of Waterloo in 1815, he again preferred to attack before his enemies could mass against him.⁷

"Divide and conquer," attributed to Julius Caesar, was another principle Bonaparte exercised repeatedly and successfully. He likely absorbed it during his youthful study, which prepared him at a level his rivals did not understand and could not match.⁸ Napoleon provides one of the best examples of the maxim that success comes to those who have put in the work of studying and learning.

Napoleon is believed to have said, "If I always appear prepared, it is because before entering an undertaking, I have meditated long and have foreseen what may occur. It is not genius which reveals to me suddenly and secretly what I should do in circumstances unexpected by others; it is thought

and preparation." If he in fact made this statement, he was simply confirming that there was no great magician's achievement in his abilities; it was meticulous effort.⁹ Unfortunately, "effort" does not sound as attractive as "genius" or "brilliance." Yet if the result of arduous work is victory, the achievement is as laudable.

A key measure of Napoleon's skill was his ability to counter the unexpected on the battlefield. He has been described as a "superb improviser."¹⁰ The ability to think quickly and respond to an unforeseen situation is a sought-after skill; in Napoleon's case, was it the result of improvisation or simply of contemplation and preparedness? Bonaparte did his homework on opponents, their armed forces, his own forces, geography, and, of course, politics.¹¹ During the Spanish campaign, he instructed French General Jean-Andoche Junot to send "descriptions of the provinces through which you pass"—one of many examples of his ceaseless drive to understand future battlefields and to master campaigns.¹²

After his initial victories in Italy, Napoleon compiled a sound basis of successful experiences around which he anchored much of his thinking.¹³ For Napoleon, success bred more success. His accomplishments provided him with a powerful sense of self-confidence as he planned future campaigns.

Operational Art and Design

Napoleon recognized the value of thought, planning, and preparedness in what he intended to do. He put into practice what today's Joint Publication (JP) 3-0, *Joint Operations*, describes as operational art and design—a "cognitive approach" that encompasses "the ability to anticipate . . . and the skill to plan, prepare, execute, and assess."¹⁴ It is further described as being "used by commanders and staffs—supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means."¹⁵ In short, success comes from thorough planning.

Napoleon stated that he had foreseen what could occur and was therefore

Table. Timeline of Napoleon's Military Career

1769	Born on the island of Corsica
1796	Campaigns in Italy
1798	Campaigns in Egypt
1804	Crowned Emperor
1805	Wins Battle of Austerlitz
1806	Wins Battle of Jena-Auerstedt
1808	Begins ongoing warfare in Spain
1812	Fails to conquer Russia
1813	Defeated at the Battle of Leipzig
1814	Exiled to the island of Elba
1815	Returns to France and begins the Hundred Days campaign
1815	Defeated at the Battle of Waterloo
1815	Exiled to the island of St. Helena
1821	Dies on St. Helena



Coronation of Emperor Napoleon I and Coronation of the Empress Josephine in Notre-Dame de Paris, December 2, 1804, by Jacques-Louis David and Georges Rouget, ca. 1805–1807, oil on canvas (Louvre Museum)

prepared if it did. His early study of operational art and design provided the advantage of insight. JP 5-0, *Joint Planning*, describes the operational art and design framework as granting an “understanding” of how to fight and win, beyond aggregate numbers of soldiers or weapons.¹⁶ The French emperor sought to out-think as well as out-fight opponents; he designed plans based on the deeper understanding his cognitive preparation had enabled.

Design “supports operational art with a methodology intended to enhance understanding of the situation and the problem.”¹⁷ JP 3-0 describes design as “the conception and construction of the framework that underpins a campaign or major [operational plan] and its subsequent execution. It extends operational art’s vision with a creative process to help commanders and planners answer the ends-ways-means-risk questions.”¹⁸ JP 3-0 notes:

Operational art and design enable understanding. Understanding is more than just knowledge of the capabilities and capacities of the relevant actors or

*the scope and nature of the [operational environment]; it provides context for decision making and how the many facets of the problem are likely to interact, enabling commanders and planners to identify hazards, threats, consequences, opportunities, and risk.*¹⁹

Operational art and design are intellectual efforts; their proficient accomplishment is anchored in experience, research, and thought. Ideally, Bonaparte’s writings would provide key clues to his use of them, but he wrote little, and much of what is believed to be his military work is tactical in nature. However, there are glimpses of operational thought.

In *Military Maxims*, he advised planning for what the enemy could do.²⁰ To Napoleon, operational design’s “understanding” was key; such planning was a contemplative effort. What are the enemy’s goals? What does the enemy value? Comprehending such matters required drawing on his knowledge and experience. Bonaparte had to place himself in his opponent’s shoes and consider his adversary’s viewpoint.

Napoleon also referenced preparedness, especially for an enemy that could appear at any time.²¹ Reconnaissance and intelligence were not yet scientific fields. The element of surprise—both Napoleon’s use of it and his preparedness for an enemy’s use of it—was an immensely powerful weapon. Preparedness at such a high level demanded vision, thought, and analysis.

Napoleon’s studiousness served him well during his early years. By 1804, he was emperor of France. He could direct his armies as he wanted²² and as emperor was not slowed by the friction of bureaucracy. He was subject only to the limits of his own decisive mind.

Action Defeats Fog and Friction

Napoleon’s successes in Italy shaped the foundation for his understanding of operational warfare. This gave him a well-developed *coup d’oeil*, or special insight, as Carl von Clausewitz described it.²³ Bonaparte’s early victories fed his instincts for battle. He used his planning skills to limit the impact of friction in war.²⁴ The more Napoleon

could contemplate scenarios and possibilities, the less likely friction would hinder the execution of his plans.

Countless commanders throughout history have succumbed to war's fog and friction. Napoleon even suffered their ill effects later in life, especially during the Hundred Days campaign in 1815.²⁵ Yet during his younger years, his skills—and his devotion of considerable time to planning and preparedness—often triumphed. History teaches that the enemy is a thinking opponent that often does not do what is expected. Bonaparte mitigated the uncertainties of war by considering various actions an enemy could take and was often prepared when they materialized.

Operational art and design teach preparedness: considering the possible and rendering it expected. Understood another way: by Napoleon's contemplation of many scenarios, he reflected on many outcomes. Although 9 of every 10

scenarios never occurred, he was prepared for the one that did.

Yet that was only half of the equation. Napoleon crafted war plans and then executed them quickly and confidently, often making the first move rather than allowing his opponents the opportunity. Speed and surprise, then, became the keys to success.²⁶ And his boldness often prevented the unexpected from occurring; decisive execution provided a chance to control events rather than to allow others to shape them. The same can be said of today's operational art and design: a successful commander is one who is likely to execute plans with speed and decisiveness,²⁷ creating an operational tempo that an opponent cannot easily overcome.

Greatest Victories

Napoleon's battlefield successes at Ulm-Austerlitz in 1805 and Jena-Auer-

stedt in 1806 display his skillful use of speed, maneuver, and the element of surprise. As the emperor might have described it, the victories could best be attributed to deep thought, planning, and aggressive execution.

Many consider the 1805 defeat of Austria and Russia the crowning example of Napoleon's skill. His multicorps attack toward Ulm completely overwhelmed the Austrians. Their commander, General Karl Mack, believed Ulm far too strong a defensive position for Napoleon to overcome.²⁸ Yet speed and resolute French actions carried the day. French corps moved decisively at rates the Austrians could not match.

Later, at the battle of Austerlitz, Napoleon's army burst through the enemy's center and pursued its left wing until it was crushed. Austerlitz was an annihilation battle for the ages. Yet these few words do not do justice to the



The Battle of Jena, October 14, 1806, by Horace Vernet, 1836, oil on canvas, depicts Napoleon reprimanding grenadier of Imperial Guard, who (according to legend) eagerly shouted for attack during Battle of Jena-Auerstedt (Palace of Versailles)

effort the French emperor put into this triumph. What historians describe as the “Battle of the Three Emperors” came down to the superior preparation and actions of just one. The French emperor, despite his troops’ being outnumbered, humbled Francis II of Austria and Alexander I of Russia on a scale that has rarely occurred. Bonaparte’s skillful drawing of the Austrians and Russians toward him and the superior French execution decided the day;²⁹ his adversaries were simply routed.³⁰ This carefully planned battle underscores the importance of operational design. Napoleon’s cleverly planned French deception and feigned weakness worked remarkably well.³¹

Andrew Roberts’s *Napoleon: A Life* recounts detailed planning for the battle of Austerlitz. Roberts describes how Bonaparte went to great lengths to ensure that his key commanders understood exactly what was expected of them in the coming battle.³² He understood that the application of the enduring principles of war coupled with speed of action made the difference on the battlefield.³³ The decisive execution of those principles was the crucial factor in his triumph; those time-tested tenets remain embedded in operational art and design today, as our joint publications demonstrate.

In fighting Prussia, Napoleon again used speed to engage and conquer his opponent quickly, before its allies might join in.³⁴ At the battle of Jena-Auerstedt, his forces fought two battles simultaneously, defeating the Prussians in both. Bonaparte relied on planning, deployed his forces, and engaged his foe. He did not use supernatural powers; it was simply his version of operational art and design.

General Bonaparte was subject to the French government during his Italian campaigns in the mid-1790s; his well-planned and speedy efforts led to victory despite this burden. In 1806, as emperor, he essentially was the French government. He engineered a rapid Prussian campaign unhindered by politics; his was the only political opinion that mattered.

Clearly, operational art is not a new concept. Claus Telp’s *The Evolution of Operational Art, 1740–1813* describes how operational art evolved during the

period from Frederick the Great through the reign of Napoleon. The 1806 Prussian campaign and Jena battle are thoroughly examined. Well documented and easy to read, the book is a mainstay of the serious study of the period.

Telp’s work, in addition to many others, also teaches that by the time of Napoleon’s campaigns, things had changed. Limited war was basically a relic of the past. The French emperor understood the transformation—and operated in a manner that simply overwhelmed Austrian, Prussian, and Russian opponents. The resulting surrenders often saw enemies accepting peace on his terms. Forcing opponents to accept peace on one’s own terms should sound familiar—it is often the goal for the United States today.

Such a goal trains the focus on operational art and design. And despite the two centuries between Napoleon’s victories and JPs 3-0 and 5-0, the through line connecting then and now is unmistakable. A study of operational art and design is perhaps the best way for today’s soldiers to understand the methods and actions of one of history’s most brilliant tacticians.

Clearly, Bonaparte was subject to the same rules of speed, maneuver, and surprise that his peers were then and commanders are today.³⁵ He simply planned and executed military campaigns faster than his contemporaries. The French emperor understood that the principles of war are timeless. They can be seen in the ancient world, in the 18th and 19th centuries, and today.

Key Lessons for Today

Historians continue to study Napoleon as if they might discover his secrets, but he simply did the deep thought and research needed. He formulated his plan, then executed it at a pace opponents could not match.³⁶ The faster warrior often secures the victory. The Prussian army in 1806 was hopelessly outclassed by the speed at which Bonaparte operated.³⁷ One hundred and thirty-four years later, the German army executed blitzkrieg at a pace the British and French could not equal.

A key lesson is that Napoleon was remarkable largely because he prepared and fought at an unmatched pace. He simply accelerated the implementation of rudimentary operational art and design; his study of the past and early victories in Italy would have taught him the value of speed. Most of Napoleon’s early foes, schooled in the 18th-century art of war,³⁸ were likely unaware of—and certainly unprepared for—his more modern skills. In analyses of Bonaparte, speed, maneuver, and surprise crop up again and again—and these studies remain relevant today because speed, maneuver, and surprise, like all other principles of war, remain relevant.

In the future, the United States may not have several years to win wars. It took the Allies 6 years to win World War II. The Gulf War, of 1991, was fought and decided in less than 6 weeks; the ground war was measured in hours. With the speed of technology today we should not expect a great deal of time to assemble victory. As former Defense Secretary Donald Rumsfeld famously said, “You go to war with the army you have, not the army you might want or wish to have at a later time.”³⁹ Future wars may be won or lost in a matter of weeks, perhaps days in extreme cases. Once a war begins, the United States will not have the time to do the required reading, deep thinking, and thorough planning. That preparation is what peace is for.

This article argues that the reading, thinking, and planning must occur now and remain ongoing. American taxpayers spend a great deal on defense. It can be argued that the United States has the best military equipment money can buy; we must spend more time on becoming the absolute best at operational art and design. We must do a great deal more reading, thinking, and planning around cyber and space in addition to the air, land, and sea domains.

Napoleon’s empire was not a democracy; his was the only opinion he cared to consult. Democracies have slower decisionmaking processes. Political leaders are often cautious with major decisions such as war, seeking the maximum possible demonstration of bipartisanship and political unity. Whereas discussion,

debate, and consensus are a blessing in most things, in war they may be a disadvantage against a peer competitor. With that warning in mind, the lessons of the French emperor become most pressing. Preparedness in art and design is essential, not least to compensate for a potentially slower political process.

The lessons here are clear: Engage fully in the study of operational art and design. Consider what an opponent might do, and be ready for multiple scenarios. War-game plans repeatedly. Ensure that plans are updated in a timely manner. If or when the time comes, be prepared to execute quickly and mercilessly.

Conclusion

Now is the time to think like Napoleon regarding future opponents and conflicts. Future conflicts will require the United States to be faster than its foes. Napoleon repeatedly demonstrated the value of speed, maneuver, and surprise. He contemplated the risk and reward and then acted decisively. The United States can ill afford to be slow in the prosecution of conflict against a peer opponent.

Now is the time to think and plan, considering ends, ways, means, and risk. As Bonaparte demonstrated, it was not sorcery but military thought and study that allowed him to accomplish so much. Once war was decided on, he prosecuted it with a zeal his foes could not match. Now is also the time to thoroughly read and review JPs 3-0 and 5-0. These documents exist for a reason: to provide direction for successful military action. They clearly direct joint activities and efforts by all the Services. Additionally, and equally important, much in these publications is essentially 21st-century Napoleonic thinking. Bonaparte would have clearly recognized in today's art and design much of how he thought about warfare.

Today, the Department of Defense should establish a formal institute of operational art and design that would encourage deeper thinking on key defense matters, with particular emphasis on operational plans. Establishing an institute, staffed by all Services and key allies, would further focus U.S. efforts

to become and remain the absolute best at art and design. It could demonstrate value by offering annual symposiums or sponsoring wargames.

Undoubtedly, the emperor's countless followers will continue to seek out his secrets. He was an incredibly talented commander and conqueror. He did well when he observed the brutal laws of war—although he strayed somewhat in later years and ultimately succumbed to his foes.⁴⁰ He may or may not have been a genius, but he was definitely a thinker, planner, and hard worker, which may have been his biggest secrets.

Napoleon at his best exercised precise planning and lightning execution, performing at a level his contemporaries did not. His work teaches today's military leaders to engage in a continuous study of operational art and design because returning to the roots of skill and professionalism is always warranted. The United States must also engineer unmatched war-winning readiness in all warfighting domains. The effort must be joint and fully integrated through operational art and design. This approach will either deter conflict or win it if deterrence fails. JFQ

Notes

¹ Frank McLynn, *Napoleon: A Biography* (London: Pimlico, 1998), 138.

² Martyn Lyons, *Napoleon Bonaparte and the Legacy of the French Revolution* (New York: St. Martin's Press, 1994), 196.

³ David G. Chandler, *The Campaigns of Napoleon* (New York: Macmillan, 1966), 138–139; McLynn, *Napoleon*, 166; Napoleon Bonaparte, *Military Maxims of Napoleon*, trans. J. Ackerly (New York: Wiley and Putnam, 1845), 67–69.

⁴ McLynn, *Napoleon*, 145.

⁵ Chandler, *The Campaigns of Napoleon*, 126–128, 136.

⁶ Lyons, *Napoleon Bonaparte and the Legacy of the French Revolution*, 197.

⁷ John Keegan, *The Face of Battle: A Study of Agincourt, Waterloo, and the Somme* (New York: Penguin, 1983), 104.

⁸ Claus Telp, *The Evolution of Operational Art, 1740–1813: From Frederick the Great to Napoleon* (New York: Frank Cass, 2005), 63–64, 67–70.

⁹ Andrew Roberts, *Napoleon: A Life* (New York: Penguin, 2014), 61, 79.

¹⁰ McLynn, *Napoleon*, 144.

¹¹ Roberts, *Napoleon*, xxxiv–xxxv.

¹² Chandler, *The Campaigns of Napoleon*, 598.

¹³ Roberts, *Napoleon*, 134–137.

¹⁴ Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017, Incorporating Change 1, October 22, 2018), II-3, available at <https://irp.fas.org/doddir/dod/jp3_0.pdf>.

¹⁵ Ibid.

¹⁶ JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), IV-1, available at <https://irp.fas.org/doddir/dod/jp5_0.pdf>.

¹⁷ JP 3-0, II-4.

¹⁸ Ibid.

¹⁹ JP 5-0, IV-1.

²⁰ Bonaparte, *Military Maxims of Napoleon*, 2.

²¹ Ibid., 9, 11–12.

²² Telp, *The Evolution of Operational Art*, 54.

²³ JP 3-0, II-1.

²⁴ JP 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, Incorporating Change 1, July 12, 2017), I-3, available at <<https://irp.fas.org/doddir/dod/jp1.pdf>>.

²⁵ Chandler, *The Campaigns of Napoleon*, 1056–1057.

²⁶ Ibid., 129–130.

²⁷ JP 5-0, IV-1.

²⁸ Todd Fisher, *The Napoleonic Wars: The Rise of the Emperor 1805–1807* (Oxford, UK: Osprey Publishing, 2001), 27–28.

²⁹ Robert Goetz, *1805: Austerlitz, Napoleon, and the Destruction of the Third Coalition* (Mechanicsburg, PA: Greenhill Books, 2005), 282–284; David G. Chandler, *Austerlitz 1805: Battle of the Three Emperors* (Oxford: Osprey Publishing, 1990), 18–20.

³⁰ Chandler, *Austerlitz 1805*, 20.

³¹ Michel Franceschi and Ben Weider, *The Wars Against Napoleon: Debunking the Myth of the Napoleonic Wars* (New York: Savas Beatie, 2008), 112.

³² Roberts, *Napoleon*, 383.

³³ Telp, *The Evolution of Operational Art*, 64.

³⁴ Ibid., 52.

³⁵ Ibid., 72.

³⁶ McLynn, *Napoleon*, 138, 145.

³⁷ Fisher, *The Napoleonic Wars*, 15–17, 22–23.

³⁸ Telp, *The Evolution of Operational Art*, 13.

³⁹ Eric Schimdt, “Iraq-Bound Troops Confront Rumsfeld Over Lack of Armor,” *New York Times*, December 8, 2004, available at <<https://www.nytimes.com/2004/12/08/international/middleeast/iraqbound-troops-confront-rumsfeld-over-lack-of.html>>.

⁴⁰ Chandler, *The Campaigns of Napoleon*, 1003–1004.



Russian President Vladimir Putin and General Valery Gerasimov observe actions of troops of Russia and Belarus at main stage of Zapad 2017 joint strategic exercises at Luzhsky training ground in Leningrad Region, September 2017 (President of Russia)

When Dragons Watch Bears Information Warfare Trends and Implications for the Joint Force

By Christopher H. Chin, Nicholas P. Schaeffer, Christopher J. Parker, and Joseph O. Janke

The predominance of the psychological over the physical, and its greater constancy, point to the conclusion that the foundation of any theory of war should be as broad as possible.

—B.H. LIDDELL HART, *STRATEGY*¹

Lieutenant Colonel Christopher H. Chin, USAF, is Branch Chief in the Future Operations Division at U.S. Cyber Command. Lieutenant Colonel Nicholas P. Schaeffer, USAF, is Chief of Intelligence aboard the National Airborne Operations Center at U.S. Strategic Command. Major Christopher J. Parker, USA, is a Strategic Planner for the Joint Staff J7 at Fort Leavenworth, Kansas. Major Joseph O. Janke, USA, is the Plans and Exercises Chief for the Eighth Army G9 in Camp Humphreys, Korea.

Over the past decade, the People's Republic of China (PRC) has watched Russia's employment of information warfare (IW) with great interest. With the recent conflict in Ukraine and the 2014 Russian annexation of Crimea, the PRC is actively gauging Western nations' response and associated global implications should it choose to forcefully reunify Taiwan. As the current pacing threat, the PRC

seeks to rewrite global norms with the intent to assert supreme influence over Taiwan and the Asia-Pacific region. The parallels between these two Great Powers and their associated aggression toward breakaway republics present an opportunity for the United States and the joint force to map the contours of an evolving Chinese information warfare strategy to build a more comprehensive U.S. response prior to a



Marine Corps Sergeant Estefany Gomez Prado, psychological operations specialist with Psychological Operations Company, 1 Marine Expeditionary Force Information Group, talks to role player during Marine Air Ground Task Force Warfighting exercise 3-22 at Marine Corps Air Ground Combat Center Twentynine Palms, California, May 1, 2022 (U.S. Marine Corps/Benjamin Aulick)

future conflict in the region. Given the scope, sophistication, and scale of modern information warfare activities, thwarting Chinese information confrontation tactics during crisis and conflict will require a comprehensive approach, one that boldly marshals increased unity of effort from across the whole of government. To compete and win in the 21st-century information environment, the Department of Defense (DOD), in partnership with the interagency community, should endeavor to lead three initiatives across upcoming joint force time horizons:

- increase the scope and scale of irregular and information warfare to better fit within the modern competition

continuum below the threshold of armed conflict (next 1 to 3 years)

- advocate to establish a central organization responsible for synchronizing U.S. whole-of-government information-related activities to counter foreign malign influence (next 3 to 5 years)
- revive service to the Nation in the digital age with the establishment of a Civilian Cyber Corps as a precursor to a seventh military branch, U.S. Cyber Force, to build the force capacity necessary to execute cyber effects operations at a scale necessary to defend the Nation, its networks, and its traditional military operations (next 5 to 7 years).

Chinese Reflections on Russian IW Activities

Much like their Chinese counterparts, Russian leaders today believe that Western democratic economic prosperity has come at their expense. The concept of *maskirovka*, or military deception, is not simply a strategic approach to conflict—rather, it is a Russian whole-of-government approach to control international perception of Russian activities to set the conditions necessary to achieve national interests.² Central to the concept of *maskirovka* are IW activities designed to distract, overload, paralyze, exhaust, deceive, divide, pacify, deter, provoke, overload, and pressure an adversary.³ These tactics can be employed

individually; however, what is compelling is the seamless orchestration of Russian IW activities with military maneuvers designed to seize the initiative, secure the element of surprise, obfuscate malicious intent, and ultimately deflect Russian attribution, thus delaying strategic consequences until it is too late for organized international response.⁴ Among the most prevalent means by which maskirovka has been executed are false flag operations, employment of proxies to engage in disinformation activities, use of private military/mercenary firms such as the Wagner Group, and employment of third-party hackers to obfuscate direct attribution to the Russian government across parts of Eastern Europe, Africa, the Middle East, and the United States. These efforts are often used in concert to prepare the environment prior to exercise or conflict.

Four major Russian exercises, which rotate between their military districts (Zapad [west], Vostok [east], Tsentral [center], and Kavkaz [Caucasus, in the Russian southern military district]), became an annual affair following the 2008 Russian army invasion of Georgia. These exercises grant Moscow flexibility to conceal its intentions and while conditioning the operational environment, enabling them to exceed the 13,000-troop limit requiring foreign observers under the Vienna Document.⁵ In almost every instance, IW activities preceded major Russian military exercises, usually playing to a “besieged castle” mentality prevalent among Russian policymakers. Russian information activities prior to Zapad 2014 (and the Russian annexation of Crimea) focused on a strategic narrative meant to cause fearful discourse—the exercise scenario depicted terrorism backed by North Atlantic Treaty Organization members Poland and Lithuania against the Russian territories of Belarus and Kaliningrad Oblast.⁶ This offered the Russians two predominant benefits in their annexation of Crimea: the ability to cast their intentions as defensive in nature based on a fictional exercise scenario and to motivate its populace into supporting a presupposed cause and effect of defending ethnic Russians in Crimea.

By comparison, China has not engaged in IW activities prior to a strategic military exercise at scale comparable to those of its northern neighbor. There is similarity in the “besieged castle” mindset, where China has crafted the threat of terrorism among its Uighur population,⁷ and the creation of laws in Hong Kong making “secession, subversion of the central government, terrorism, or collusion with foreign forces punishable by up to life in prison.”⁸ China has used this narrative to great effect and is now poised to learn even more from Russia, recently hosting Russian troops for joint strategic drills inside the PRC for the first time.⁹

As authoritarian governments, both China and Russia have successfully demonstrated a willingness and ability to coordinate IW activities across their whole of government. These regimes have the mechanisms to execute a deliberate information campaign to achieve ends that conflict with international norms and expectations for responsible conduct by civilizations in the 21st century. The United States is disadvantaged in this realm and should be concerned that Russia and China are taking steps to learn more from each other to counter Western influence in their respective spheres of influence.

Chinese IW Lessons Learned

Chinese propagandists have studied Russian techniques of flooding the information space with false narratives and wish to emulate Russian success in influencing U.S. actions and sentiment. A concept in Chinese political discourse called *huayu chizi* references a deep-seated feeling that China is maligned or, worse, ignored during global discussion and debate.¹⁰ The remedy to this is strengthening its own *wai xuan*, or external messaging (propaganda) to spread the PRC message in a positive light. To execute this plan, Chinese media leadership described the use of media outlets such as Russia Today (RT) as an “external propaganda aircraft carrier” that should be used to affect social media and break through foreign media environments.¹¹ A 2018 *People’s Daily* article noted favorably that RT

had a sizable and growing presence on Facebook, Twitter, and YouTube, as well as a vast growing network of media partnerships across the globe. Furthermore, Russian media strategy was summarized as being a two-part unified strategy: one, presenting a positive expression of Russian views and perspectives on world events, and two, displaying Russian culture and the nation in a positive light. Although the Chinese analysts noted that *wai xuan* would not be the decisive factor in altering sentiment in the West, it would counter negative narratives and add dissonance to anti-Chinese media narratives.¹²

There is also a growing overt acknowledgment that Russian lessons learned are worth studying by Chinese propagandists. Russia and China have held an annual “Internet Media Cloud Forum” since 2015. The most recent iteration occurred in late 2020 and featured keynote speeches by the editor in chief of *China Daily* and the Russian deputy minister of digital development, communications, and mass media. This gathering was focused on increasing Chinese-Russian communication via new information technologies such as artificial intelligence, so-called big data, and 5G telecommunication systems. In addition, Russian and Chinese leaders pledged to build media cooperation by creating “media innovation research centers” and “talent exchange” products—processes widely understood to create a pathway for Russian information techniques to filter into Chinese operations.¹³ Although cooperation is still limited, the connection has been established. While it is likely that Russian actions could not be copied perfectly by Chinese IW specialists, there are undeniable signs of learning and adopting Russian techniques, particularly RT’s success in presenting and amplifying “alternative” views to Western audiences.

This position is also being advocated in publicly available Chinese research journals. Writing admiringly about Russian information operations targeted to the West, one author explains how “external communication power” is an important part of the country’s soft power. In recent years, China has also





Chinese President Xi Jinping boards aircraft carrier *Shandong* and reviews guards of honor at naval port in Sanya, Hainan Province, December 17, 2019 (Xinhua/Li Gang)



Ukrainian President Volodymyr Zelensky autographs Ukrainian flag for frontline troops during visit to defensive lines, December 20, 2022, in Bakhmut, Donetsk Oblast, Ukraine (Ukrainian Presidential Press Office)

been continuously strengthening its external communication capabilities to model RT's success in penetrating the Western mind. Russia's national system and information processes have created an increasingly complete and unique international communication system.¹⁴ In late 2015 the Sputnik Chinese News Service was officially launched; it successively opened Weibo and WeChat public accounts to increase official and unofficial cooperation between Russian and Chinese state-run media. In 2015, RT also signed a cooperation agreement with the China News Agency to carry out long-term cooperation on joint interviews and news events.

More concerning is the growing Chinese military boldness in the South China Sea and other areas, spurred by Beijing's perception of being in a "period of strategic opportunity."¹⁵ The PRC is implementing an approach that

is uncannily Russian in growing its reach and strategic positioning through actions below the threshold of activating the international community against China or provoking the United States into military conflict.

There are specific ways in which the Chinese media environment observed Russian actions in Crimea and absorbed associated lessons. First, during the preparation period for the war of public opinion, RT described the agenda in economic terms and avoided political terms to prevent comparisons to European and American Cold War attitudes. This presages Chinese activity in the South China Sea—China is only "securing trade routes" and "ensuring Chinese economic zones are respected." Second, during the rising period of conflict, Russian media shifted the topic from economic to political, describing anti-Russian protesters as rioters and terrorists and invoking a dual

dilemma of political crisis and economic crisis. This connecting of political ends via economic justification is also very clear in Chinese justification of territorial growth in international waters. Third, Russia continued to use historical and democratic arguments to reduce international willingness to intervene, citing arguments such as "This is what the people want" and "This land has always belonged to Russia," which Chinese propagandists are actively using to justify a huge range of military and economic encroachments along its southern shores. These arguments, the author notes, are particularly effective against Western leaders because they come (often falsely) within a framework of democratic ideals and upholding the right of people to self-govern.

Undoubtedly, the PRC has studied the information environment in the lead-up to and throughout the 2022 Russian invasion of Ukraine. Chinese strategists

are likely formulating narratives to counter the Joseph R. Biden administration's skillful use of intelligence disclosures, such as the proactive "prebttal" aimed at shaping global opinion against the Russian buildup leading to its invasion of Ukraine in February 2022.¹⁶

A Better Appreciation for Competition

Combating such nuanced and pervasive information warfare activities requires a greater understanding of the modern competition continuum and how DOD engages our adversaries below the threshold of armed conflict. Such an understanding not only makes clear the PRC's comprehensive, whole-of-government approach to competition, but also reveals the current shortcomings of our bifurcated joint approach to competition that stifles creativity and inhibits combatant commander initiative. Joint Doctrine Note 1-19 (JDN 1-19), *Competition Continuum*, describes competition below armed conflict as nonviolent actions conducted by the joint force or proxies to achieve objectives that are mutually at odds with those of a competitor.¹⁷ Acknowledging that competition requires the whole of government, JDN 1-19 distinguishes between the instruments of national power and those actions reserved specifically for the joint force. At the top, competition consists of "diplomatic and economic activities, political subversion, intelligence and counterintelligence, operations in cyberspace and the information environment, [and] military engagement," while the joint force is left with "security cooperation, military information support, freedom of navigation, and other nonviolent military engagement activities."¹⁸ These separate spheres, and the narrow focus left for the joint force, stand in sharp contrast to the holistic approach espoused by the People's Liberation Army (PLA) and its "Three Warfares" strategy.

Nestled within the PLA's broader strategy of "active defense" is an operational concept uniquely suited for the offense during competition below armed conflict. As the cornerstone of China's

global influence operations, the Three Warfares strategy employs psychological warfare, public opinion warfare, and legal warfare to promote a pro-Beijing narrative and set conditions for achieving outcomes favorable to the Chinese Communist Party's strategic objectives.¹⁹ The concept relies on propaganda, deception, threats, and coercion to affect adversary decisionmaking, while propagating targeted narratives and disinformation in public forums to sway key domestic and international audiences.²⁰ Although its methods are relatively standard, what the Three Warfares concept lacks in ingenuity, it makes up for in scale and scope, effectively bridging the gap between party, state, army, and populace in a distinctly Chinese version of unified action. The United Front Work Department, Propaganda Ministry, State Council Information Office, PLA, and Ministry of State Security are all key actors in a coordinated effort to influence audiences at home and abroad.²¹ Acknowledging the breadth and coordination inherent in the Three Warfares concept provides a benchmark for recognizing just how much the joint force must adapt and where it should start if it is to effectively compete with the PRC. Below are four recommendations that will allow the U.S. joint force to prevail in modern warfare.

Recommendation 1: Greater Incorporation of Irregular Warfare & Information Warfare Concepts.

To prevail in Great Power competition (GPC), the United States must abandon its myopic view of war and peace as two sharply distinct states in favor of a broader understanding that includes innovative ways and means of operating below the threshold of armed conflict. The foremost way DOD can do this is by redefining irregular warfare to better incorporate information warfare activities to provide the joint force with the tools necessary to operate across the competition continuum.

The current DOD definition of irregular warfare is too narrow to remain relevant in an era defined by GPC. Joint Publication 1 defines *irregular warfare* as "a violent struggle among state and non-state actors for legitimacy and influence

over the relevant population(s)."²² Irregular warfare is distinguished from traditional warfare by its non-Westphalian character—its disregard for the norms surrounding state sovereignty and internal affairs. Much like information warfare, irregular warfare approaches are often indirect or asymmetric, tailored to protracted conflicts, and designed to "erode their opponent's power, influence, and will."²³ Both Russia and China practice irregular warfare and information warfare approaches below the level of armed conflict, actively employing their forces to undermine or delegitimize a competitor by controlling the narrative, confusing the situation, and influencing key audiences.

While the overall concept remains viable, the term *violent* in the definition of irregular warfare betrays its intent and is in need of revision. The definitional constraint that describes irregular warfare as a violent struggle limits its conduct to only periods of armed conflict and is a vestige of antiquated U.S. military thinking that embraced a narrow peace-war dichotomy inconsistent with the integrated campaigning model presented in the competition continuum.²⁴ Campaigning through cooperation, competition, and conflict addresses adversaries who view competition as a constant, uninterrupted struggle for "security, influence, and resources."²⁵ However, operating along the continuum requires the appropriate tools, and just as "little green men" sowed confusion in Ukraine and "little blue men" made de facto claims to disputed reefs in the South China Sea, the joint force needs creative irregular warfare options it can employ during both competition and conflict.

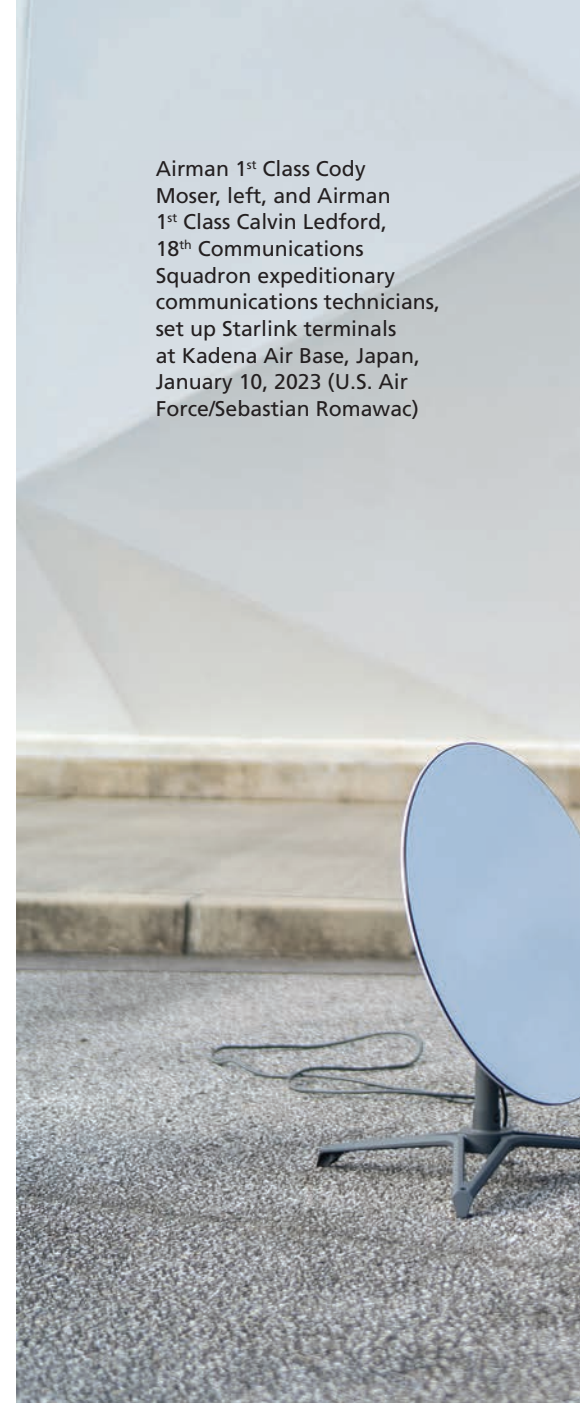
Although simple, revising the definition of irregular warfare to expand its applicability acknowledges the changing character of warfare reflected in contemporary doctrine, provides greater options for commanders competing below the level of armed conflict, and drives the creativity necessary to prevail in GPC. This is not a call to change policy or authorities but is instead a way of changing how the joint force understands and integrates irregular warfare and

information warfare activities in unison below the level of armed conflict. Recent publications such as JDN 1-19 recognize the changing character of warfare and the need to adapt the joint force's approach to competition. Current revisions to Joint Publication 5-0, *Joint Planning*, both highlight the importance of campaigning through competition and emphasize the necessity of multi-domain tactics in 21st-century warfare. Key terms, such as *decisive point*, have been revised to address operations in cyberspace, and likewise, *irregular warfare* should be updated to account for its expanded utility during periods of persistent competition.²⁶ Other scholars have made similar arguments, pointing to the need for an improved understanding of unconventional warfare (UW)—an irregular warfare mission area—to better compete by disrupting or coercing a competitor.²⁷ Instead of focusing primarily on support to insurgencies, advocates argue that UW should be plied actively in the information environment, fomenting unrest or coercing adversarial governments. While this change aligns with the position presented here, it is but a part of the cultural shift required to broaden how the joint force understands competition.

Expanding the definition of *irregular* beyond the confines of armed conflict provides combatant commanders with the option of conducting activities usually restricted to a joint operations area or joint special operations area, on an enduring basis, and without the need for national command authority approval, so long as these activities are primarily focused on subverting an adversary's ability to expand its influence within a combatant commander's theater of operations below the level of armed conflict. This expansion aligns with similar discussions surrounding the delegation of authorities for offensive cyber operations that occurred during General Paul Nakasone's Senate confirmation hearing in 2018. In his written testimony, General Nakasone argued that "Based on the evolving nature of adversary cyber capabilities and threats, USCYBERCOM [U.S. Cyber Command] must be postured to defend the Nation in and through cyberspace,

which may necessitate conducting certain cyber activities and operations outside of armed conflict or declared areas of hostilities."²⁸ So too must combatant commanders have the ability to conduct irregular warfare activities below the level of armed conflict; whether through operational preparation of the environment or UW. With this expanded purview, both irregular warfare and information warfare activities can be built into theater campaign plans and will no longer be reserved strictly for contingencies. This will invigorate planning and provide commanders with even more options for campaigning through cooperation, competition, and conflict.

Recommendation 2: Whole-of-Government Approach, Revive the U.S. Information Agency. The U.S. engagement in the information domain cannot be limited to the exclusive capabilities of a single department nor be siloed in its approach. Our adversaries have demonstrated an ability to craft strategic narratives that span the national instruments of power and employ them to great effect. While our current efforts have increased, we cannot expect to compete or dominate until we achieve unity of effort and, ideally, unity of command, in our information campaign. In 1999, years after our victory in the Cold War, we dismantled the U.S. Information Agency (USIA), as there was a perception it was no longer needed. As a result, we lost the ability to marshal the combined effort of our departments under a single Cabinet-level representative who had a "seat at the table" with our nation's leadership.²⁹ Today, the National Security Council attempts to fill the void of crafting the "position of the Nation" often lacking a unified voice that an established Cabinet-level representative with associated resources would afford. We would implore the Nation's leadership to revisit the idea of a U.S. Information Agency, updated and expanded for the 21st century and the current era of GPC, with the expanded mission of countering foreign malign influence. This cannot be a single department effort or the USIA of the past—the organization must be staffed in an integrated fashion with



Airman 1st Class Cody Moser, left, and Airman 1st Class Calvin Ledford, 18th Communications Squadron expeditionary communications technicians, set up Starlink terminals at Kadena Air Base, Japan, January 10, 2023 (U.S. Air Force/Sebastian Romawac)

those background in the professions of arms, intelligence, law enforcement, and statecraft. DOD would provide members who can assist with crafting and countering strategic narratives and who are knowledgeable about the three stages of narrative creation: formation (how narratives are created), projection (how narratives are spread and contested), and reception (how narratives are received) if we want to "stick the landing."³⁰ Greater emphasis should be placed on creating an environment where State Department action officers are integrated with a blend of Servicemembers with backgrounds



in foreign area operations (political or regional affairs strategists), information operations, influence operations, public affairs, strategy, intelligence, and cyber warfare. Many who challenge the recreation of a USIA will say that this was an institution designed for a simpler time of bipolarity (United States versus Soviet Union, or “West versus the Rest”), when the world was less digitally connected. With its rebirth, a modern USIA would be charged with marshaling the whole-of-government response to countering foreign disinformation campaigns by consolidating the authorities and capabilities

resident in DOD, the Department of Justice, the Department of State, and the Department of Homeland Security under a single organization to operate seamlessly to counter foreign disinformation threats to the United States.

Recommendation 3: Building and Retaining a National Cyber Force. In 1933, Franklin D. Roosevelt enacted the New Deal, consisting of a series of workforce programs designed to not only revitalize the Nation’s workforce but also restore the competitive advantage of the United States. A key aspect of the New Deal centered on an initiative called the

Civilian Conservation Corps (CCC), a program focused on recruiting, training, employing, and ultimately reinvigorating a young cadre of Americans whose sole focus would be to rebuild, restore, and preserve the Nation’s critical infrastructure, Federal lands, and natural resources during a time of domestic turmoil and global uncertainty.

Today, the Nation is at an inflection point whereby Americans’ science, math, engineering, and digital literacy is eroding at an alarming rate compared with that of our PRC competitor. And despite billions of dollars’ worth of

investments in the information technology and security programs, DOD is unable to generate the capacity required to cover in totality the scope and scale of espionage and cyber attacks posed by our Great Power adversaries.

Much like the CCC in 1933, DOD could take the lead in revisiting what service to the Nation looks like (beyond today's traditional uniformed armed Services) in the 21st-century information age, especially in technical fields of computer engineering, information technology, and cyber security. In that scenario, the Nation would be formulating the means to harness the voluntary energy of technically gifted patriotic American citizens at a young age, with minimal investment. Much as the CCC of the past provided the core of the U.S. Army's noncommissioned officer corps during World War II, an information-centric version of the CCC would offer a means for our nation's technically gifted to serve in a reserve "Civilian Cyber Corps" and to be called on to augment the defense of critical infrastructure sectors in a time of national crisis. Recent events have shown that neither DOD nor the U.S. Government has the capacity or skill sets to effectively secure our nation's cyberspace and critical infrastructure sectors from cyber attacks. The establishment of a Civilian Cyber Corps would be a worthy investment, enabling the Nation to rapidly cultivate young technical talent while simultaneously providing an avenue for service to the country.

Taking a note from history, a Civilian Cyber Corps would be centered on establishing a framework whereby our nation's technical talent could be cultivated at an early age and offered streamlined pathways to serve their nation outside of a traditional military uniformed Service framework. A Civilian Cyber Corps would bolster the means to support the DOD's Defense Support to Civil Authorities mission with leadership predominantly coming from the Reserves or National Guard due to the components' strong ties to industry, along with partnerships to establish the connective tissue necessary to defend and secure the Nation at the state and Federal

levels. It would offer not only technical training but also employment, from basic information systems administration to something as advanced as malware analysis and threat heuristics.

Structurally, the Civilian Cyber Corps would be focused on three broad lines of effort, consisting of recruitment, development, and integration into existing Federal and state cyber security organizations. From a recruitment and development standpoint, the Civilian Cyber Corps would focus on developing digital literacy and cultivating technical talent along a broad spectrum of sectors, from grade school youths all the way to young adults under 25 years old. Much like the Boy Scouts of America, participants of the program would be incentivized by technical training opportunities, Federal grants, academic scholarships, and even streamlined appointments to participating U.S. military academies and participating universities later on, if participants demonstrated continued interest and dedication. Upon graduation, participants would be offered internships in technology companies, government sectors, and, if they should so choose, appointments to the Armed Forces Reserves, designed to be called on in times of national emergency such as a cyber attack on critical infrastructure or to support key national-level cyber initiatives. From an integration standpoint, the Civilian Cyber Corps would offer maximum capacity to serve across Federal, state, and local governments, and potentially private-sector organizations. A modern Civilian Cyber Corps would create a "digital bench" for our Federal and state leaders to recruit and draw from as a means to resource and even lead the multitude of cyberspace and information technology across the national security apparatus. Now more than ever, the Nation needs bold ideas and creative methods to cultivate, recruit, and ultimately employ the full extent of its technical prowess to address 21st-century information age challenges. The establishment of a Civilian Cyber Corps would revolutionize service to the Nation in the 21st century while sparking the competitive spirit of young

Americans outside of traditional military service that is needed to win against our nation's Great Power adversaries.

Finally, the establishment of a Civilian Cyber Corps would help DOD formulate the precursor and establishment of a seventh military branch—U.S. Cyber Force—a Service dedicated solely to organizing, training, and equipping offensive and defensive cyber forces to defend the Nation, secure its networks, and support its traditional military activities. The Civilian Cyber Corps could be a natural feeder into this new military Service, one that starts the recruitment and development of digital talent at a young age for service to the Nation. Also, a Civilian Cyber Corps would provide a natural Reserve Component for those who seek respite from Active duty and would like to seek opportunities outside the military while still serving in a limited capacity. It is time for DOD to recognize that since the establishment of the Cyber Mission Forces (USCYBERCOM's action arm), the force's readiness, capacity, and retention have steadily declined while the requirements placed on these low-density and high-demand forces continue to increase. The way each military Service organizes, trains, and equips our cyber forces is currently disjointed, cumbersome, overly bureaucratic, and ultimately lacks institutional support for greater resourcing, since cyber operations is not each of the Services' primary mission. Countless congressional hearings centered on the retention of cyber professionals have proved that the mechanisms we have in place—whether they are cyber-excepted service for civilians or direct commissioning mechanisms into the Armed Services—have proved to be both insufficient and unable to scale to meet the demands placed on the force. Much as there is a need to establish an organization dedicated to recruitment and development of digital talent at a young age by way of a Civilian Cyber Corps, so is there a need for the U.S. military to have a separate and distinct Service dedicated to the organization, training, and equipping of cyber warfare forces if we want to build a force that is postured to fight and win in the information environment.

Conclusion

In the face of unprecedented challenges and threats to our democracy, we must be prepared to take bold actions at this critical juncture in our nation's history. The recent convergence of Russian and Chinese actions in the information space proves that the risk of inaction is far too great. Initiative loss in this arena is rarely recoverable, and its impact will span generations of Americans and democratic nations around the world now and into the future. The competition continuum is vast and complex, and it extends far beyond DOD's authorities alone.

The time for courageous new approaches is now. We must implement swift changes to antiquated ideologies that handcuff the joint force's ability to maneuver in this dynamic battlespace. Therefore, we believe DOD must expand its definition of irregular warfare to reflect a modern competition continuum, advocate with our interagency partners to build a central U.S. information agency, and finally, establish a new framework for service to the Nation outside the traditional uniformed Services. This would be accomplished through the establishment of a Civilian Cyber Corps, which would leverage our nation's digital talent for the national defense and would act as a means to build a future United States Cyber Force. Together, these reforms will enable the joint force to maintain its competitive edge over our adversaries today and protect the values at the heart of our nation's democracy in the future. JFQ

Notes

¹ Basil Henry Liddell Hart, *Strategy*, 2nd ed. (New York: Signet, 1974), 5.

² Conor Cunningham, "A Russian Federation Information Warfare Primer," The Henry M. Jackson School of International Studies, November 12, 2020, available at <<https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/>>.

³ Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no. 2 (2004), 237–256.

⁴ Brenna Cole and George Noel, "Nation-

State Perspectives on Information Operations and the Impact on Relative Advantage," paper presented at the International Conference on Cyber Warfare and Security, February 2021.

⁵ Dave Johnson, "ZAPAD 2017 and Euro-Atlantic Security," *NATO Review*, December 14, 2017, available at <<https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html>>.

⁶ Andreas Ventsel et al., "Discourse of Fear in Strategic Narratives: The Case of Russia's Zapad War Games," *Media, War & Conflict* 14, no. 1 (March 2021), 24–26.

⁷ Sheena Chestnut Greitens, Myunghee Lee, and Emir Yazici, "Understanding China's 'Preventive Repression' in Xinjiang," *Order From Chaos* (blog), March 4, 2020, available at <<https://www.brookings.edu/blog/order-from-chaos/2020/03/04/understanding-chinas-preventive-repression-in-xinjiang/>>.

⁸ "Hong Kong Security Law: Anger as China's XI Signs Legislation," BBC, June 30, 2020, available at <<https://www.bbc.com/news/world-asia-china-53234255>>.

⁹ Tom O'Connor, "China Hosts Russia Troops to Hold Strategic Military Drills for First Time," *Newsweek*, August 2, 2021, available at <<https://www.newsweek.com/china-hosts-russia-troops-hold-strategic-military-drills-first-time-1615496>>.

¹⁰ Elizabeth Chen, "China Learning From Russia's 'Emerging Great Power' Global Media Tactics," *China Brief* 21, no. 7 (April 12, 2021), available at <<https://jamestown.org/program/china-learning-from-russias-emerging-great-power-global-media-tactics/>>.

¹¹ Ibid.

¹² Kristin Huang, "Can Beijing Use Lessons Learned by Europe to Ease South China Sea Tensions?" *South China Morning Post*, November 9, 2019, available at <<https://www.scmp.com/news/china/diplomacy/article/3036788/can-beijing-use-lessons-learned-europe-ease-south-china-sea>>.

¹³ Chen, "China Learning From Russia's 'Emerging Great Power' Global Media Tactics."

¹⁴ Gary Rawnsley, "To Know Us Is to Love Us: Public Diplomacy and International Broadcasting in Contemporary Russia and China," *Politics* 35, nos. 3–4 (2015), 273–286, available at <<https://doi.org/10.1111/1467-9256.12104>>.

¹⁵ *China's Military Power: Modernizing a Force to Fight and Win* (Washington, DC: Defense Intelligence Agency, 2019), 4–140.

¹⁶ Jake Harrington, "Intelligence Disclosures in the Ukraine Crisis and Beyond," *War on the Rocks*, March 1, 2022, available at <<https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/>>.

¹⁷ Joint Doctrine Note (JDN) 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), 4–7, available at <<https://www.jcs.mil/Portals/36/>

Documents/Doctrine/jdn_jg/jdn1_19.pdf>.

¹⁸ Ibid., 2.

¹⁹ *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020* (Washington, DC: Office of the Secretary of Defense, 2020), 130, available at <<https://media.defense.gov/2020/sep/01/2002488689/-1/-1/1/2020-dod-china-military-power-report-final.pdf>>.

²⁰ Ibid.

²¹ Ibid.

²² Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, Incorporating Change 1, July 12, 2017), I-6, available at <<https://irp.fas.org/doddir/dod/jp1.pdf>>.

²³ Ibid.

²⁴ JDN 1-19, *Competition Continuum*, 4–7.

²⁵ Blagovest Tashev, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* 10, no. 2 (2019), 141, available at <<https://dx.doi.org/10.21140/mcu.2019100208>>.


²⁶ JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), IV-32, available at <https://irp.fas.org/doddir/dod/jp5_0.pdf>.

²⁷ Otto C. Fiala and Jim Worrall, "Imposing Costs: Unconventional Warfare in the Information Environment," *Modern War Institute*, July 6, 2021, available at <<https://mwi.usma.edu/imposing-costs-unconventional-warfare-in-the-information-environment/>>.

²⁸ Senate Armed Services Committee, Advance Policy Questions for Lieutenant General Paul Nakasone, USA, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 115th Cong., 2nd sess., 2018, 31, available at <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf>.

²⁹ Dr. Vivian Walker, email, July 22, 2021, following author's presentation, "Countering Disinformation Narratives: Strategic Approaches," Joint Combined Warfighting School, Norfolk, VA, July 16, 2021.

³⁰ Alister Miskimmon, Ben O'Loughlin, and Laura Roselle, *Forging the World: Strategic Narratives and International Relations* (Ann Arbor: University of Michigan Press, 2017).



Air Force's 10th Wideband Global SATCOM communications satellite, atop United Launch Alliance's Delta IV rocket, lifts off from Space Launch Complex 37B at Cape Canaveral Air Force Station, Florida, March 15, 2019 (U.S. Air Force/Van Ha)

Mind the Gap

Space Resiliency Advantages of High-Altitude Capabilities

By Benjamin Staats

Adversaries continue to pursue new, improved, and expanded counterspace capabilities to target and exploit the perceived reliance by the United States and its allies

Major Benjamin Staats, USA, is a Future Operations Planner at U.S. Space Command. He originally wrote this article while a Schriever Space Scholar at the Air Command and Staff College.

on space-based systems.¹ Furthermore, adversaries continue to strengthen and expand antiaccess/area-denial (A2/AD) strategies designed to disrupt or degrade warfighting command systems so as to slow or otherwise deter the U.S. military from protecting its interests.² Since 2010, the United States has attempted to mitigate these growing threats by pursuing a strategy of improving space architecture resiliency.³

However, neither space systems nor space capabilities and their effects have attained a level of resiliency commensurate with the existing and emerging threats. To remedy this lingering deficiency, then-Chief of Space Operations General John W. Raymond stated that the top priority of the U.S. Space Force in 2022, and probably for the next decade, was to shift to a more resilient architecture.⁴

This more resilient architecture must include cross-domain capabilities, specifically high-altitude systems, to improve overall capability and mission resiliency and better enable a Joint All-Domain Command and Control (JADC2) framework that achieves greater warfighting mission assurance in a heavily contested and complex operational environment (OE). Although improving the resiliency of space-based architecture alone is an important effort to assure space capabilities and their missions and effects, it should not be the only means. As part of this deterrence-by-denial strategy, the joint force should concurrently develop high-altitude capabilities to improve space mission resiliency, better assure warfighting mission requirements, and better enable the joint force to accomplish its objectives. These high-altitude capabilities can fill critical operational gaps and requirements anticipated to emerge in a future contested OE. Integrating and layering them into existing tactical and operational organizations, networks, and frameworks will help to offset the vulnerabilities and disadvantages of both space and air assets.

The counterspace threat and need for a resilient architecture resemble conditions faced by the newly independent British Royal Air Force (RAF) during the interwar period. The anticipated air threat from France, and later Germany, compelled the RAF to develop a more efficient and highly organized air defense command and control (C2), communications, and intelligence architecture.⁵ The emergence of radar provided a critical battlefield intelligence capability that the RAF was able to rapidly integrate into an already developing architecture.⁶ Not only did the improved air defense architecture initially help deter Germany from planning to invade Great Britain, the integration of radar proved to be a critical factor in the country's successful defense during the Battle of Britain. Just as radar served as a critical capability to improve the RAF's air defense C2, communications, and intelligence architecture, high-altitude capabilities can serve as critical enablers to improve space architecture, mission resiliency, and JADC2 for the U.S. joint force.⁷

This article argues that the joint force must develop high-altitude capabilities and integrate them into joint operations to improve space mission resiliency. High-altitude capabilities ensure that warfighting mission requirements are met and will enable the joint force to achieve its objectives in a conflict when adversaries attempt to heavily contest both air and space. The following section recommends a joint definition for the high-altitude region, continues with a historical review of the development and importance of high-altitude capabilities, describes how their use will improve space mission resiliency, and concludes with recommendations for ways the joint force should develop and budget for these important high-altitude capabilities as it prepares for the next conflict.

Defining the High-Altitude Region for Joint Doctrine

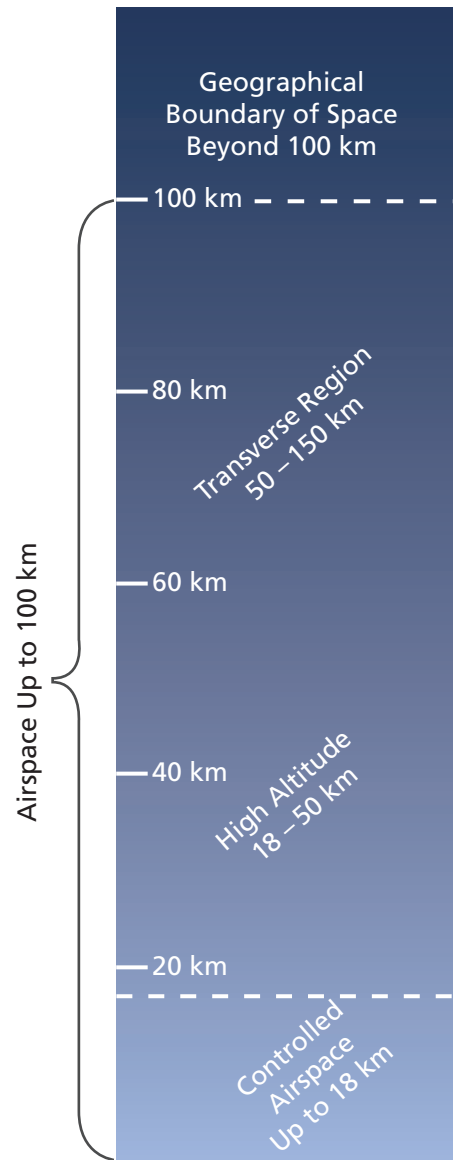
Joint doctrine needs to provide clear operational definitions for the extended regions between traditionally exploited airspace and outer space. A portion of upper airspace remains undefined despite having significantly different physical attributes from those of both space and the airspace traditionally exploited by aircraft. Without a definition of this part of the OE in joint doctrine, there is a lack of clarity and shared understanding, particularly as technology further enables the potential for capabilities to exploit these regions.

The figure illustrates a proposed concept for delineating the distinct regions of airspace leading up to the geographical boundary of space at 100 kilometers. This high-altitude region is bounded by two well-established demarcations: the ceiling of controlled airspace, at roughly 18 km (60,000 feet), and the beginning of the transverse region, at roughly 50 km (164,000 feet).

Lower Boundary of High Altitude.

The Federal Aviation Administration (FAA) officially considers anything above 18 km as upper-class E airspace and provides no airspace management services for the range of high-altitude capabilities that operate within it.⁸ Further, given the lower density of air molecules at higher

Figure. Undefined Regions Between Air and Space



altitudes, only a few traditional air assets, such as the Global Hawk and the U-2, have the capacity to reach beyond controlled airspace.⁹ As a result, the airspace region above 18 km remains largely vacant and unexploited by anything other than nontraditional air platforms, such as high-altitude balloons or aerostats.

Upper Boundary of High Altitude.

The unique principles of physics beyond 50 km, aptly named the transverse region, permit only the act of traversing it, primarily via rockets and missiles. Essentially, the transverse region lies between air and space, where neither aerodynamic flight nor orbital rotation is possible.¹⁰ The

physical upper boundary of high-altitude systems seems to be at the beginning of the transverse region, roughly 50 km, given operational testing thus far. In 2018, the National Aeronautics and Space Administration's record-breaking test demonstrated a high-altitude balloon could sustain altitude at roughly 49 km.¹¹

Given these demarcations, neither the Department of the Air Force's nor the Department of the Army's definition is suitable. The U.S. Air Force unofficially defines the near-space region as between 20 km and 99 km, but this definition seems too broad, given that the upper 49 km of this region is distinctly different from the part below 50 km.¹² More recently, the U.S. Army has defined the high-altitude region as between roughly 18 and 30 km (specifically, 60,000 to 100,000 feet).¹³ However, whereas the unofficial Air Force definition is too broad, the Army's is too restrictive, considering the potential for some high-altitude assets to reach well beyond 30 km. Thus, to establish a shared understanding of what is meant by the high-altitude region, joint doctrine should define it with boundaries at 18 km and 50 km.

Besides defining its boundaries, another way to understand and frame the high-altitude region is to consider it a littoral zone between airspace and outer space. Just as the U.S. Navy has increasingly determined the importance of littoral zones in its operations, so too should the joint force consider the importance of the high-altitude region for achieving greater resiliency.

Taking Insights From History

Much as Sputnik triggered the beginning of the space age in 1957, the first human flight in an untethered balloon in 1783 sparked the era of "balloomania" across the United States and Europe.¹⁴ Just 10 years later, a French military hydrogen balloon called *L'Entreprenant* floated above several battles in the 1890s to relay detailed aerial reconnaissance information to the commanding general.¹⁵ Both civil and military balloon activity carried on throughout the 19th century, and a segment of balloonists competed

seriously for altitude records well into the 20th century.¹⁶ By 1935, the record altitude had reached over 21 km, far beyond the record-breaking 6 km established in 1803 and well into what is now considered the high-altitude region.¹⁷ While the airplane overshadowed the value of balloons throughout most of the 20th century, the utility of balloons reemerged once they could reach altitudes unachievable by modern airplanes.

By the early 1950s, unmanned balloons, as part of the Navy's Helios and Skyhook projects, could achieve altitudes greater than 30 km.¹⁸ This achievement spurred further high-altitude balloon research, engineering, and experimentation in the 1950s and 1960s, including strategic reconnaissance.¹⁹ Most historians, in focusing on President Dwight D. Eisenhower's choice of the U-2 spy plane as the near-term stopgap solution for accurate intelligence on the Soviet nuclear threat until the United States could deploy reconnaissance satellites overlook the complementary high-altitude balloon programs.²⁰ For example, the Air Force developed the Moby Dick program to deploy high-altitude balloons equipped with cameras from Okinawa, Hawaii, and Alaska starting in January 1956 as part of a weather balloon cover plan called White Cloud.²¹ In a 6-month period before the first U-2 flight over the Soviet Union, more than 250 high-altitude balloons recorded approximately 8 percent of the territory of the Soviet Union and China before they were discovered and a diplomatic spat ensued, leading to the program's termination.²²

Overshadowed by the effectiveness of new air and space capabilities, the utility of high-altitude balloons did not emerge again until the 21st century. In response to observed operational shortfalls in Operation *Iraqi Freedom* (OIF) and Operation *Enduring Freedom* (OEF), the Air Force tasked Air Force Space Command (AFSPC) to develop, field, and execute tactical and operationally responsive space capabilities that included high-altitude capabilities (also described as "near-space" capabilities).²³ Despite

the potential utility described by most Air Force research and experiments from 2005 to 2007, the Service was unable and unwilling to adequately pursue and fund high-altitude capabilities.²⁴ Ultimately, high-altitude capabilities were not required to address the immediate threat at that time.

Since then, the Air Force, the Navy, and the Army have increasingly pursued variations of high-altitude capabilities to fill niche operational gaps, particularly in response to emerging counterspace threats. However, the resurgence of interest in high-altitude capabilities fostered extravagant development programs, with unreasonable demands, untested technologies, and inexperienced developers all driving toward an ill-defined and disjointed problem set.²⁵ As a result, the inevitable failures of most of these programs have facilitated and exacerbated the poor reputation of high-altitude capabilities. For example, the Army unrealistically expected to develop the long-endurance multi-intelligence vehicle (LEMV) within just 18 months, but after spending \$297 million and dealing with significant program mismanagement, the Pentagon finally terminated the program.²⁶ The LEMV failure highlights how high-altitude capabilities failed as a wartime innovation because of insufficiently stated requirements and a narrowly defined problem set that became increasingly irrelevant as OIF and OEF war efforts began to draw down.²⁷

Instead, the joint force should seek to innovate high-altitude capabilities during periods of relative peace and Great Power competition but make sure to appropriately guide research and development (R&D) by anticipating the operational gaps and future requirements based on emerging threats.²⁸ Potential adversaries, such as China and Russia, continue to train and equip their military space forces with increasingly sophisticated and extensive counterspace weapons to hold the space assets of the United States and its allies and partners at risk.²⁹ Further, these developments enhance Chinese and Russian A2/AD strategies that continue to advance and accelerate in ways that will challenge joint all-domain operations.³⁰ This



Operators and engineers launch high-altitude balloon as part of U.S. Pacific Fleet's Unmanned Systems Integrated Battle Problem 21, Warner Springs, California, April 25, 2021 (U.S. Navy/David Mora)

evolving and expanding threat creates an increasingly complex OE that may exceed the threshold of near-future air- and space-based support capacities.

Given the anticipated and evolving threat, the joint force must develop and integrate high-altitude capabilities into joint operations to improve the resiliency of space missions during conflict. These systems will help assure warfighting requirements that enable the joint force to achieve its objectives despite the expected degradation or loss of space-based capabilities.

Improving the Resiliency of Space Missions With High-Altitude Capabilities

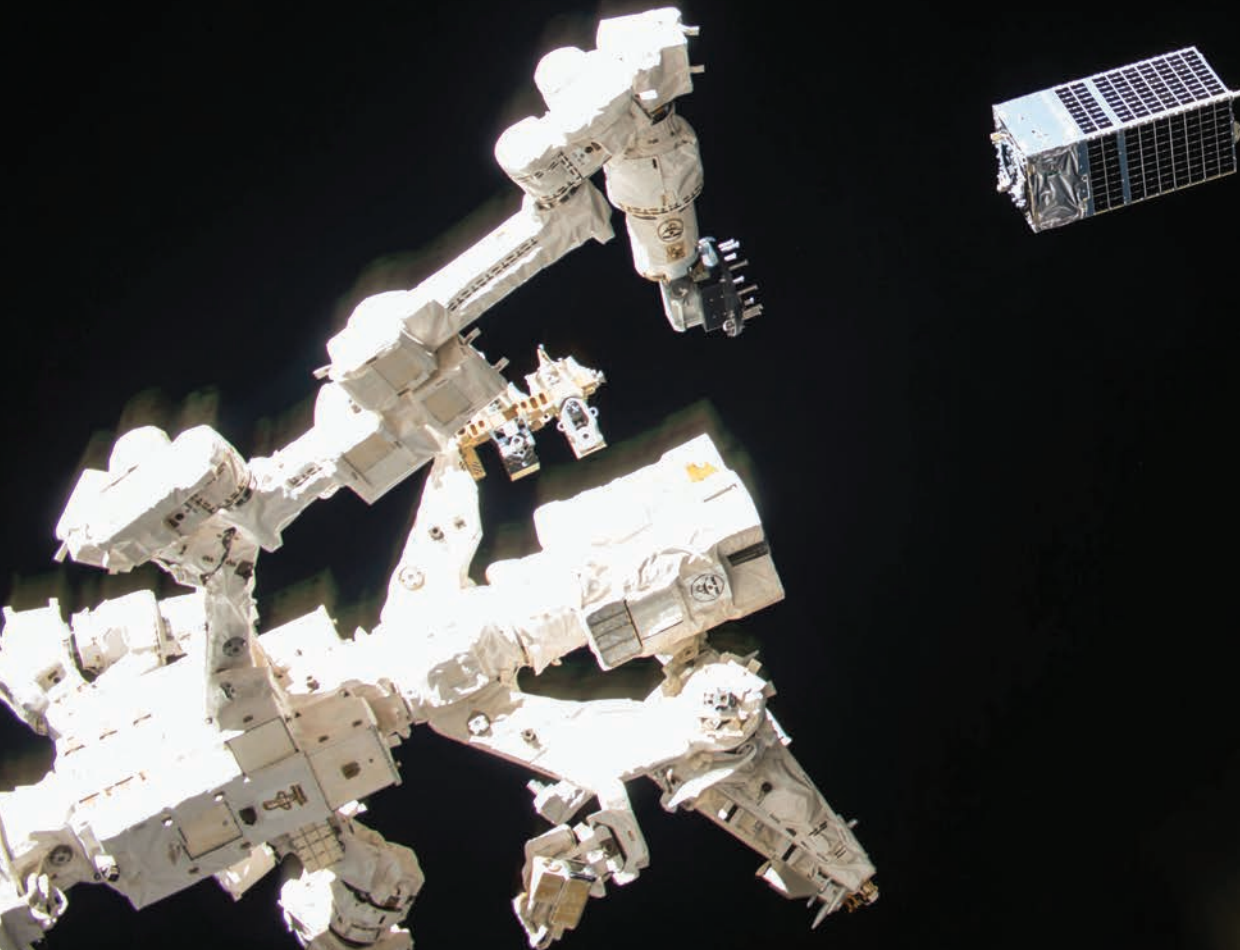
Strengthening the resiliency of the U.S. space architecture has been a key national-level space policy objective since 2010.³¹ However, in 2016, the RAND Corporation noted that the prioritization of space resiliency by senior military leadership had not been promulgated formally down to space squadrons.³² In December 2015, the Office of the Secretary of Defense recognized issues with discussing, implementing, and measuring space resilience

efforts.³³ Further, AFSPC's 2015 Space Enterprise Vision study recognized the ongoing need to improve space architecture resiliency.³⁴ The AFSPC commander at the time, General John Hyten, later stated that the Space Enterprise Vision opposed "any of those big, exquisite, long-term satellites."³⁵

Senior leadership across the Department of the Air Force stated in 2022 that increasing space resiliency is a top priority.³⁶ Specifically, General Raymond expressed the same concern General Hyten had when he stated that "we [need to shift] from a handful of exquisite capabilities that are very hard to defend to a more robust, more resilient architecture."³⁷ Despite some improvements over the years, the primary problem remains: space capabilities are not resilient enough, and it may take several more years to attain a more resilient space architecture. Further, attaining a degree of space resiliency commensurate with the emerging and evolving threat may be unfeasible with a space-domain-specific approach alone. In other words, the joint force needs more than just space systems resiliency; it needs space mission resiliency and assurance.

High-altitude capabilities can serve as critical cross-domain resiliency alternatives that fill the anticipated operational gaps and meet future operational requirements as the joint force attempts to further strengthen the resiliency of its space architecture and develop a robust JADC2 framework. Although domain-specific space architecture resiliency is important to assure space mission availability, it cannot be the only means to improve the overall resiliency of the space missions needed to assure warfighting requirements.³⁸ Integrating and layering high-altitude capabilities into existing tactical and operational organizations, networks, and frameworks to complement existing and future air and space capabilities can improve the much-needed resiliency of space missions and, ultimately, warfighter mission assurance. The joint force will need this sort of redundancy and resiliency to fill anticipated capability and capacity gaps in a future contested OE.³⁹

High-altitude capabilities can improve resiliency because they can generate and provide space-like effects from altitudes above traditionally exploited airspace yet well below the threshold of



Kestrel Eye—low-cost, visible-imagery satellite prototype designed to provide near-real-time images to tactical-level ground Soldier—was launched to International Space Station as payload aboard SpaceX Falcon 9 from Kennedy Space Center in Florida, August 14, 2017, and deployed into space and activated on October 24, 2017 (U.S. Army Space and Missile Defense Command Technical Center/U.S. Army Acquisition Support Center)

space. By no means can, or should, high-altitude capabilities replace proven air and space capabilities, but they do provide an array of advantageous attributes, such as responsiveness, persistence, and field of view. The unique combination of these attributes helps offset inherent disadvantages and limitations in existing air and space capabilities. Although none of the individual attributes are unique to high-altitude capabilities, the brief summaries below will begin to illustrate how layering and integrating them into air and space architectures can help improve resiliency of space missions to enable warfighter mission assurance and enhance joint operations.

Responsiveness. The joint force can quickly launch and task high-altitude capabilities across the joint area of operations (JOA). Existing high-altitude systems have already demonstrated

the ability to fill and launch from their launch platforms within 30 minutes from austere locations and in winds up to 45 knots while requiring a relatively minimal logistics footprint.⁴⁰ After launch, high-altitude systems can reach their altitudes within an hour or so and can be tasked throughout their ascents, and the payloads can be detached and recovered by means of technologies similar to those integrated into joint precision airdrop systems.⁴¹ Launches can also occur well outside the JOA or from logistics and support hubs, though it could take several hours or days for the systems to drift into position, depending on the distance. In addition, the joint force could have a great number of these systems launched from across varying tactical and operational echelons.

Once high-altitude capabilities are in place, software advances have made

them mostly autonomous, interoperable, and maneuverable, enabling the joint force to place them into positions of advantage or standoff.⁴² In a complex, contested, and rapidly changing OE, these attributes could allow tactical- and operational-level commanders immediate, potentially on-demand access to alternate intelligence, surveillance, and reconnaissance (ISR), as well as communications, missile warning, and other capabilities typically provided by air and space assets. Further, these commanders could directly reallocate, reposition, or retask dedicated tactical high-altitude systems according to mission requirements, instead of reallocating strategic air and space assets.

Persistence. High-altitude capabilities can also provide persistent coverage over an entire JOA, given their unique loitering and endurance abilities. Existing

high-altitude platforms have demonstrated the ability to maintain relative stability for weeks within acceptable loitering positions using little energy, by manipulating the winds to adjust their altitudes and to maneuver.⁴³ This degree of persistence is enabled by emerging technologies such as the stratospheric optical autocovariance wind lidar and the adaptable lighter-than-air balloon. These systems demonstrate the ability for high-altitude systems to maintain their loitering and altitude positions up to 27 km for weeks at a time.⁴⁴

Given their persistence, these systems can achieve staring effects, like space capabilities in geostationary orbit, albeit vastly closer. This staring effect enables the joint force to integrate a unique and persistent ISR and communications capability that complements air and space capabilities in addition to filling gaps in a contested OE. Further, high-altitude systems are also relatively all-weather systems; they operate above the troposphere, where most terrestrial weather occurs. And commanders can deploy high-altitude capabilities in a proliferated manner to attain greater reliability for on-demand tasking.

Field of View. Given their high altitudes above the JOA, high-altitude capabilities can achieve large fields of view, up to a few hundred miles wide. Although not nearly as large as those achieved by satellites, high-altitude capabilities' fields of view are greater than those of traditional air platforms. For example, a high-altitude system can achieve a field of view of 400 miles across from an altitude of 100,000 feet.⁴⁵ In addition, a high-altitude system at 90,000 feet can image at a 45-degree off-nadir angle from up to 18 miles of horizontal standoff, whereas an MQ-1 at 25,000 feet and an MQ-9 at 50,000 feet can achieve approximately only 5 and 10 miles of horizontal standoff, respectively. The more expansive fields of view of high-altitude capabilities also enable them to extend beyond-line-of-sight communications from two to eight times the range attainable by unmanned aerial vehicles.⁴⁶

Although the field of view of high-altitude capabilities pales in comparison to that of satellites, their proximity to

terrestrial targets provides significant advantages. For example, the same lightweight optical sensors used on small satellites would generate significantly better image resolution—well beyond the 3- to 5-meter resolution achieved from low Earth orbit—if employed on high-altitude systems. The field of view achieved by high-altitude capabilities also enables a range of advantages for ISR, communications, missile warning, and other missions that greatly benefit tactical- and operational-level commanders.

The attributes discussed above represent only some of their advantages; there is clear significant value to layering high-altitude systems with existing air and space capabilities to improve resiliency of space missions that assure warfighter mission requirements. The joint force will not always be able to maintain total dominance in all domains.⁴⁷ High-altitude capabilities could fill the potential capacity and capability gaps created in a contested OE. For example, the responsiveness, persistence, and field of view attributes of high-altitude capabilities would enable reliable, all-weather, space-like ISR and communications across the JOA.

First, high-altitude ISR sensors can provide higher resolution and greater signal sensitivity relative to more costly space assets—and offer larger fields of view and endurance relative to air assets.⁴⁸ The ability to collect real-time imagery, information, and signal data across the battlefield would greatly enhance the decisionmaking process for commanders. The provided space-like ISR support could enhance the joint force's ability to confirm and deny priority information requirements, improve tracking and targeting processes, and generate a better shared understanding of the OE to help validate common operating pictures and contribute to the iterative planning process. Thus, not only would high-altitude ISR capabilities ensure greater space mission resiliency, they also could complement existing air and space capabilities and fill the potential gaps in ISR coverage in a competitive OE.

Second, high-altitude communications assets could serve as reliable primary,

alternate, contingency, or emergency means of over-the-horizon communications within a contested OE. These platforms could expand and supplement existing joint C2 capabilities by serving as relays or repeaters capable of extending ground-based radio signals several hundred miles across the JOA.⁴⁹ Communication payloads would decrease the burden and risk to existing satellite communications (SATCOM) architectures by reducing user capacity requirements, offloading certain data signals, or relaying SATCOM signals to mitigate jamming attempts.⁵⁰ As high-altitude capabilities became more stable, they could also serve as ideal platforms to exploit free-space optical communications, particularly within a contested OE. Last, high-altitude communications positioned below the ionosphere could fill a capability gap when space weather hazards, such as shortwave radio fade and signal fade, occur.⁵¹

Although many more mission areas are promising for improving the resiliency of space missions, such as ongoing high-altitude missile-warning capabilities, the high-altitude-based ISR and communications alternatives provide two examples of opportunities for greater cross-domain resiliency that ultimately could assure warfighter mission requirements. High-altitude capabilities could not only enable greater cross-domain resiliency, they could also enable the joint force to allocate, prioritize, and preserve low-density, high-demand air and space assets more efficiently throughout operations—a key function of effective C2.⁵² Further, during Great Power competition, the joint force deployment of high-altitude capabilities, particularly in a proliferated manner, would present an additional dilemma to an adversary by altering operational patterns and force posture while creating opportunities for the joint force to exploit adversary operational shortfalls.⁵³ In short, there would be many benefits to the joint force in pursuing high-altitude capabilities. The next section presents a discussion of how to move forward to take advantage of this region and exploit the gap.

U-2 from Beale Air Force Base, California, prepares to land at Royal Air Force Fairford, England, June 9, 2015 (U.S. Air Force/Jarad A. Denton)

Developing and Integrating Deliberate High-Altitude Capabilities

Before discussing how the joint force should more deliberately pursue the development and integration of high-altitude capabilities, senior leaders must understand why integrating high-altitude capabilities previously failed. Their development in the past two decades was a response to wartime requirements and thus was a wartime innovation effort. Unfortunately, historical lessons indicate that wartime innovation is possible, but often unsuccessful and imperfect, and, when successful, available only in the later phases of a war.⁵⁴ Wartime innovation takes time, and during war, time is short.⁵⁵ Capabilities not developed prior to war are often imperfectly cobbled together during conflict because military organizations often fail to identify and develop clear and concise warfighter requirements to meet objectives, to effectively establish or train a new organization to employ newly developed capabilities, or to sufficiently go through a wartime learning process to measure the capabilities' strategic effectiveness.⁵⁶

The wartime innovation effort of integrating high-altitude capabilities in the 21st century experienced these same challenges. Despite some R&D prior to OIF and OEF, it was not until after a few years of war that military organizations sought to deliberately pursue the development and integration of high-altitude capabilities to meet their operational requirements. Then, because such programs take time to develop, there were no military organizations organized, trained, or equipped to effectively employ the new capacities, and uncontested air and space capabilities often overshadowed their utility, making it difficult to measure their true effectiveness. Thus, when scrutinized, the integration of high-altitude capabilities became an apparent wartime innovation failure that did not account for all aspects of doctrine, organization, training, materiel, leadership and education, personnel, and facilities. A clear example is the previously discussed LEMV; wartime innovation challenges directly contributed to its failure.

As the RAF's air defense network did with its integration of the radar innovation during relative peacetime, a resilient space mission framework must integrate

new capabilities to attain cross-domain resiliency. If the joint force is certain that adversaries in the next conflict will contest space and air capabilities to impede its ability to achieve its objectives, then the force should deliberately pursue peacetime innovation efforts to develop and integrate high-altitude capabilities to improve space mission resiliency. Pursuing greater space mission resiliency now would give the joint force the necessary time to identify how high-altitude capabilities could improve resiliency, to establish the required organizations or processes to integrate those capabilities, and to conduct exercises, training, and wargaming to measure their effectiveness.

If the joint force commits to pursuing high-altitude capabilities during relative peacetime to prepare for the next conflict, it must address two significant challenges: organizational resistance and cost-effectiveness. The history of organizational resistance in the U.S. military to balloons dates to the Civil War, when it took a directive from President Abraham Lincoln to establish the Army Aeronautics Corps.⁵⁷ That organizational resistance remained largely entrenched until the innovation of the airplane rendered it moot. Given the utility of



integrating modernized balloons today at higher altitudes, organizational resistance, like that to any innovation, is a significant barrier. Despite this resistance, the U.S. Army Space and Missile Defense Command (USASMDC) remains committed to developing high-altitude capabilities that can enable the joint force to accomplish its objectives.⁵⁸


USASMDC is uniquely postured to further develop and integrate high-altitude capabilities into the joint force because of its organizational acceptance and because it is organized to do so effectively across the joint force. First, USASMDC serves as the proponent for Army space operations officers (FA40s) and high-altitude capabilities doctrine as part of Army space doctrine. Second, these FA40s serve at division, corps, and Army Service Component Command Space Support Elements and at 1st Space Brigade as part of Army space control planning teams, all of which support combatant commands (CCMDs) and participate in joint theater-level strategic and operational exercises, Army warfighter exercises, project convergence, and national training centers. Third, this degree of joint integration presents multiple opportunities for FA40s to integrate

high-altitude capabilities into joint operations and in coordination with joint staffs at CCMDs and the air operations center, as part of the combined space tasking order and, during exercises or conflict, the air tasking order.⁵⁹ This approach leverages an organization that already accepts high-altitude capabilities to further expand their integration into the joint force and measure their effectiveness at improving space mission resiliency, in addition to complementing air and space capabilities when training in a contested OE.

To address the challenge of cost-effectiveness, the joint force and its senior leaders must recognize that only high-altitude capabilities can achieve the cross-domain space mission assurance needed for the next conflict. When the Army developed the previously discussed LEMV to provide additional ISR to the theater commander, it was not cost-effective, given that air and space capabilities could readily meet most of those ISR requirements.⁶⁰ Because the next conflict will heavily contest air and space capabilities, the real value of high-altitude capabilities will be their ability to improve resiliency of space missions with space-like effects that enable warfighter mission assurance. Thus, if the joint force

values such benefits from cross-domain resiliency, it should invest in high-altitude capabilities appropriately.

A common argument in support of high-altitude capability development is that it is significantly less expensive than satellites, costing approximately \$100,000 per balloon in initial development and operating costs.⁶¹ However, for the joint force to gain the space resiliency needed with these types of systems, it would likely need to deploy hundreds of these balloons, or even more expensive systems, up to \$9 million, in a proliferated manner within a large JOA or across multiple JOAs.⁶² Although this employment method raises the costs, the joint force's investment of tens of millions of dollars into high-altitude capabilities would be cost-effective because it would achieve greater space mission resiliency. Although this cost assessment makes high-altitude capabilities seem less appealing in comparison to developmental satellites, such as the USASMDC Kestrel Eye, which cost approximately \$2 million apiece, the joint force must deploy Kestrel Eye in a proliferated manner across low Earth orbit and reconstitute it annually to gain any space resiliency.⁶³ And even if high-altitude capabilities approached the cost of a proliferated satellite constellation, they



United Launch Alliance Atlas V rocket carrying 6th Space Based Infrared System Geosynchronous Earth Orbit satellite launches from Space Launch Complex 41, on Cape Canaveral Space Force Station, Florida, August 4, 2022 (U.S. Space Force/ Joshua Conti)

would provide significantly more value to the joint force, given the greater gain in the requisite cross-domain space mission resiliency needed for the next conflict.

Conclusion

There are challenges to exploiting the gap with high-altitude capabilities, but the joint force can overcome them. The U.S. Space Force's efforts to improve space architecture resiliency with space-domain-specific solutions alone are not a comprehensive solution for the emerging counterspace threat. The joint force and Services must identify an organizational lead to develop and integrate high-altitude capabilities into joint operations. Although the Space Force could be the entity to exploit this gap, it probably has significant organizational resistance—something USASMDC has already overcome.

In addition, although high-altitude capabilities may be more costly than they initially appear, the resiliency benefits they provide the joint force make them a cost-effective solution to a clearly defined requirement. Commercial high-altitude capabilities could be an option, but only the joint force can generate the demand for them. Although commercial space capabilities can thrive without government funding, commercial high-altitude capabilities can thrive only with government program commitment, as is true of many other military-specific capabilities.

Given the emerging threat as the joint force prepares for the next conflict and the utility of high-altitude capabilities for improving space mission resiliency, the joint force should mind the gap between air and space. Integrating high-altitude capabilities across this gap and into joint operations would improve space mission assurance and JADC2 by providing persistent and responsive ISR and communications across the JOA, which would assure warfighting mission requirements and enable the joint force to accomplish its objectives. Further, exploiting this gap with high-altitude capabilities would complicate the adversary's ability to deny, degrade, or disrupt space capabilities because of the proliferation, redundancy,

and rapid reconstitution that high-altitude capabilities can provide. These capabilities can play a critical role in future deterrence-by-denial strategies.

Just as the RAF took care to leverage the full range of capabilities to improve its C2 architecture in preparation for war, the joint force should mind the gap and leverage high-altitude capabilities to improve its space architecture resiliency as it prepares for the next conflict. **JFQ**

Notes

¹ *Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion* (Washington, DC: Defense Intelligence Agency, 2022), iv, 40, available at <www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf>.

² John J. Klein, *Understanding Space Strategy: The Art of War in Space* (New York: Routledge, 2019), 86–87.

³ *National Space Policy of the United States of America* (Washington, DC: The White House, June 28, 2010), 9, available at <https://history.nasa.gov/national_space_policy_6-28-10.pdf>; *National Security Space Strategy: Unclassified Summary* (Washington, DC: Department of Defense and Office of the Director of National Intelligence, January 2011), 10–11, available at <https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf>.

⁴ Theresa Hitchens, “Space Force’s Top Priority for Next Decade: Resiliency, Says CSO Raymond,” *Breaking Defense*, March 3, 2022, available at <<https://breakingdefense.com/2022/03/space-forces-top-priority-for-next-decade-resiliency-says-cso-raymond/>>.

⁵ Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), 15–16.

⁶ *Ibid.*, 15–18.

⁷ *Ibid.*, 15.

⁸ *Upper Class E Traffic Management Concept of Operations*, vers. 1.0 (Washington, DC: Federal Aviation Administration, May 2020), 1, available at <https://nari.arc.nasa.gov/sites/default/files/attachments/ETM_ConOps_V1.0.pdf>.

⁹ Loren Thompson, “U-2 Versus Global Hawk: Why Drones Aren’t Always the Best Solution for Warfighters,” *Forbes*, February 5, 2018, available at <<https://www.forbes.com/sites/lorenthompson/2018/02/05/u-2-versus-global-hawk-why-drones-arent-always-the-best-solution-for-warfighters/#6f2278264d7e>>. Designers of

the Global Hawk and U-2 often refer to them specifically as high-altitude capabilities.

¹⁰ M.V. Smith, *Ten Propositions Regarding Spacepower* (Maxwell AFB, AL: Air University Press, October 2002), 38, available at <https://media.defense.gov/2017/may/05/2001742913/-1/-1/0/fp_0009_smith_propositions_regarding_spacepower.pdf>.

¹¹ Doris Elin Urrutia, “This Giant, Ultrathin NASA Balloon Just Broke an Altitude Record,” *Space.com*, September 12, 2018, available at <<https://www.space.com/41791-giant-nasa-balloon-big-60-breaks-record.html>>.

¹² Les Doggrell, “Operationally Responsive Space: A Vision for the Future of Military Space,” *Air and Space Power Journal*, Summer 2006, 44. The U.S. Space Force and U.S. Space Command have also yet to define these regions.

¹³ Field Manual (FM) 3-14, *Army Space Operations* (Washington, DC: Headquarters Department of the Army, October 2019), 1–10, available at <https://irp.fas.org/doddir/army/fm3_14.pdf>.

¹⁴ Alexander Rose, *Empires of the Sky: Zeppelins, Airplanes, and Two Men’s Epic Duel to Rule the World* (New York: Random House, 2020), 23.

¹⁵ Charles Coulston Gillispie, *Science and Polity in France: The Revolutionary and Napoleonic Years* (Princeton, NJ: Princeton University Press, 2004), 372; Caren Kaplan, “The Balloon Prospect: Aerostatic Observation and the Emergence of Militarised Aeromobility,” in *From Above: War, Violence, and Verticality*, ed. Peter Adey, Mark Whitehead, and Alison J. Williams (London: C. Hurst & Co., 2013), 25–26.

¹⁶ Craig Ryan, *The Pre-Astronauts: Manned Ballooning on the Threshold of Space* (Annapolis, MD: Naval Institute Press, 1995), 39.

¹⁷ *Ibid.*, 9, 39.

¹⁸ *Ibid.*, 68.

¹⁹ *Ibid.*, 5–9, 68.

²⁰ Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age* (Baltimore, MD: The Johns Hopkins University Press, 1997), 113, 117; David N. Spires, *Beyond Horizons: A Half Century of Air Force Space Leadership*, rev. ed. (Maxwell AFB, AL: Air Force Space Command in association with Air University Press, 1998), 31, 39.

²¹ Curtis Peebles, *The Moby Dick Project: Reconnaissance Balloons Over Russia* (Washington, DC: Smithsonian Institution Press, 1991), 163.

²² Ryan, *The Pre-Astronauts*, 68–69. Just over 500 balloons were launched, and only half were recovered, meaning that much more than 8 percent could have been recorded had the other half of the balloons and their payloads been recovered.

²³ Kurt D. Hall, *Near Space: Should Air Force Space Command Take Control of Its Shore?* Maxwell Paper No. 38 (Maxwell AFB, AL:

Air War College, September 2006), vii–viii, available at <<https://apps.dtic.mil/sti/pdfs/ADA460177.pdf>>.

²⁴ See Edward B. Tomme, *The Paradigm Shift to Effects-Based Space: Near-Space as a Combat Space Effects Enabler*, Research Paper No. 2005-01 (Maxwell AFB, AL: Air University, 2005), available at <<https://apps.dtic.mil/sti/pdfs/ADA434352.pdf>>; Hall, *Near Space*, viii.

²⁵ Anthony Tingle, “When the Balloon Goes Up: High-Altitude for Military Application,” *Military Review*, May–June 2019, 71–72.

²⁶ W.J. Hennigan, “Army Lets Air Out of Battlefield Spyship Project,” *Los Angeles Times*, October 23, 2013, available at <<https://www.latimes.com/business/la-xpm-2013-oct-23-la-fi-blimp-fire-sale-20131023-story.html>>.

²⁷ Rosen, *Winning the Next War*, 22–38, 180–182.

²⁸ *Ibid.*, 60–75, 253–254.

²⁹ Statement of Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, Testimony Before the Senate Select Committee on Intelligence, 115th Cong., 2nd sess., February 13, 2018, 17, available at <<https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA--Unclassified-SSCI.pdf>>; Todd Harrison et al., *Space Threat Assessment 2020* (Washington, DC: Center for Strategic and International Studies, March 2020), 5, available at <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200330_SpaceThreatAssessment20_WEB_FINAL1.pdf?6sNra8FsZ1LbdVj3xY867tUVu0RNHw9V>.

³⁰ TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, December 6, 2018), vi–vii, available at <<https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf>>; FM 3-14, *Army Space Operations*, v.

³¹ *National Space Policy*, 9; *National Security Space Strategy*, 10–11.

³² Gary McLeod et al., *Enhancing Space Resilience Through Non-Materiel Means* (Santa Monica, CA: RAND Corporation, 2016), 49, available at <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1067/RAND_RR1067.pdf>.

³³ *Space Domain Mission Assurance: A Resilience Taxonomy* (Washington, DC: Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, September 2015), 1, available at <<https://man.fas.org/eprint/resilience.pdf>>.

³⁴ “Hyten Announces Space Enterprise Vision,” U.S. Air Force, April 13, 2016, available at <<https://www.af.mil/News/Article-Display/Article/719941/hyten-announces-space-enterprise-vision/>>.

³⁵ Sandra Erwin, “STRATCOM Chief Hyten: ‘I Will Not Support Buying Big Satellites That Make Juicy Targets,’”

Space News, November 19, 2017, available at <<https://spacenews.com/stratcom-chief-hyten-i-will-not-support-buying-big-satellites-that-make-juicy-targets/>>.

³⁶ Hitchens, “Space Force’s Top Priority for Next Decade”; Opening Statement of Mr. Frank Calvelli, Nominee for Assistant Secretary of the Air Force for Space Acquisition and Integration, Senate Armed Services Committee, 117th Cong., 2nd sess., April 2022, available at <<https://www.armed-services.senate.gov/imo/media/doc/Calvelli%20Opening%20Statement%20Final.pdf>>; Charles Pope, “Kendall Outlines ‘Operational Imperatives,’ Choices During Think Tank Appearance,” U.S. Air Force, January 19, 2022, available at <<https://www.af.mil/News/Article-Display/Article/2904711/kendall-outlines-operational-imperatives-choices-during-think-tank-appearance/>>.

³⁷ Sandra Erwin, “Raymond: Space Force in 2022 to Focus on the Design of a Resilient Architecture,” *Space News*, January 18, 2022, available at <<https://spacenews.com/raymond-space-force-in-2022-to-focus-on-the-design-of-a-resilient-architecture/>>.

³⁸ David G. Perkins and James M. Holmes, “Multidomain Battle: Converging Concepts Toward a Joint Solution,” *Joint Force Quarterly* 88 (1st Quarter 2018), 54, available at <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88_54-57_Perkins-Holmes.pdf?ver=2018-01-09-102340-943>.

³⁹ Tingle, “When the Balloon Goes Up,” 69.

⁴⁰ “Secure, Reliable, and Ubiquitous Wireless Communications,” *Space Data*, available at <<https://spacedata.net/>>; “Loon: Expanding Internet Connectivity With Stratospheric Balloons,” X, available at <<https://x.company/projects/loon/>>; Jennifer Antoine, “Marines Expand Communication Range with Combat SkySat,” Defense Visual Information Distribution Service, March 30, 2012, available at <<https://www.dvidshub.net/news/86047/marines-expand-communication-range-with-combat-skysat>>.

⁴¹ “Scientific Balloons FAQs,” National Aeronautics and Space Administration, available at <<https://www.nasa.gov/scientificballoons/faqs>>.

⁴² Nick Statt, “Alphabet’s Loon Sets Its Sights on the Satellite Industry,” *The Verge*, January 31, 2019, available at <<https://www.theverge.com/2019/1/31/18200879/alphabet-project-loon-sdn-networking-technology-telesat-satellite-deals>>.

⁴³ Nathan Mattise, “Project Loon Team Gave Puerto Rico Connectivity—and Assembled a Helicopter,” *Ars Technica*, February 18, 2018, available at <<https://arstechnica.com/science/2018/02/project-loon-engineer-sees-a-tool-for-future-disaster-response-in-puerto-rico/>>; Loren Grush, “World View Keeps One of Its High-Altitude Balloons Afloat for a Full 16 Days,” *The Verge*, June 5, 2019, available at <[world-view-enterprises-stratollite-balloon-high-altitude-satellites>.](https://www.theverge.com/2019/6/5/18653106/</p></div><div data-bbox=)

⁴⁴ David Hambling, “The U.S. Military Is Testing Stratospheric Balloons That Ride the Wind So They Never Have to Come Down,” *MIT Technology Review*, November 14, 2018, available at <<https://www.technologyreview.com/2018/11/14/139092/darpa-is-testing-stratospheric-balloons-that-ride-the-wind-so-they-never-have-to-come-down/>>.

⁴⁵ “Secure, Reliable, and Ubiquitous Wireless Communications.”

⁴⁶ Tomme, “The Paradigm Shift to Effects-Based Space,” 25; “Secure, Reliable, and Ubiquitous Wireless Communications.”

⁴⁷ Perkins and Holmes, “Multidomain Battle,” 55.

⁴⁸ Tomme, “The Paradigm Shift to Effects-Based Space,” 11–12.

⁴⁹ “Secure, Reliable, and Ubiquitous Wireless Communications.”

⁵⁰ Tomme, “The Paradigm Shift to Effects-Based Space,” 26, 64.

⁵¹ FM 3-14, *Army Space Operations*, 2-14, 6-4.

⁵² Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, October 22, 2018), I-12, III-2.

⁵³ TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 15.

⁵⁴ Rosen, *Winning the Next War*, 179–182.

⁵⁵ *Ibid.*, 181.

⁵⁶ *Ibid.*, 180–182.

⁵⁷ Charles M. Evans, *War of the Aeronauts: A History of Ballooning in the Civil War* (Mechanicsburg, PA: Stackpole Books, 2002), 86–87.

⁵⁸ “High Altitude,” U.S. Army Space and Missile Defense Command, available at <https://www.smdc.army.mil/Portals/38/Documents/Publications/Fact_Sheets/HA.PDF>.

⁵⁹ JP 3-14, *Space Operations* (Washington, DC: The Joint Staff, April 10, 2018, Incorporating Change 1, October 26, 2020), IV-6, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf>.

⁶⁰ John Cummings, “Long Endurance Multi-Intelligence Vehicle (LEMV) Agreement Signed,” U.S. Army, June 17, 2010, available at <https://www.army.mil/article/41024/long_endurance_multi_intelligence_vehicle_lemv_agreement_signed>.

⁶¹ Tingle, “When the Balloon Goes Up,” 72.

⁶² Dave Long, “CBP’s Eyes in the Sky,” U.S. Customs and Border Protection, April 11, 2016, available at <<https://www.cbp.gov/frontline/frontline-november-aerostats>>.

⁶³ Kenneth J. Bocam et al., “Kestrel Eye Block II,” paper presented at the 32nd Annual AIAA/USU Conference on Small Satellites, Logan, UT, August 4–9, 2018, 1–2, available at <https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4103&context=small_sat>.

U.S. Army barge, powered by outboard motors, crosses Irrawaddy River near Tiggyiang, Burma, with Soldiers, ammunition, and truck, December 30, 1944 (U.S. Army/William Lentz)



Echoes of the Past

The Burma Campaign and Future Operational Design in the Indo-Pacific Region

By Shane Williams, John Green, Richard Kovsky, and Edwin Sumantha

When you go home, Tell them of us and say, For your tomorrow, We gave our today.

—War Memorial at Kohima

Lieutenant Colonel Shane Williams, USAF, is the Executive Officer of U.S. Transportation Command J3, Scott Air Force Base, Illinois. Captain John Green, USN, is the U.S. Special Operations Command J8 Lead Assessment Director, Tampa, Florida. Colonel Richard Kovsky, USAF, is Chief of the Open Skies Department at the Defense Threat Reduction Agency. Colonel Edwin Sumantha, Indonesian Army, is the Staff Director of the Indonesian Army Command and General Staff College.

The literature, personal accounts, and films documenting World War II over the past 80 years have generally overlooked a pivotal chapter of that conflict: the 1942–1945 Burma



Scouting detachment of armed Burmese patriot fighters, accompanied by two American Soldiers, cautiously wades through jungle stream in Northern Burma, circa 1944 (Chronicle/Alamy)

campaign. The few accounts that exist describe this “forgotten war” as one of the most remote, demanding, lengthy, and heroic struggles of the war.¹ They tell stories of overcoming catastrophe to reach triumph, replete with leadership failures and successes, innovations in warfare and operational art, and astonishing endurance and courage. These stories offer poignant lessons for the U.S. joint force today. The interaction of technology, readiness, and tactical concepts in Burma provides inferences for the contemporary relationships among these factors. These inferences lead to implications for joint force operational design. Future Indo-Pacific battlefields require operational designs that stress proficiency over mass and firepower, emphasize maneuver and sustainment in contested environments, and leverage allies and partners against monolithic opponents. Joint force leaders must actively practice operational art and continually adapt these designs to recover quickly from losses and capitalize on

success. Despite the passage of time, the Burma campaign provides penetrating insights into how the joint force may prevail in a contemporary conflict in the Indo-Pacific region.

This article is organized into three parts. First, a historical narrative of the Burma campaign highlights the struggles of 1942–1943, then details the second Arakan operation, the second Chindit operation, the battle of Imphal-Kohima, and the final Allied operation to retake Burma. Second, inferences are drawn from the historical narrative applied to modern warfare. Finally, implications for future joint force operational design in the Indo-Pacific derive from these inferences, indicating lessons contemporary joint force commanders and staffs can learn from the Burma campaign.

The Campaign

1942–1943. In his stirring account of the Burma campaign, Field Marshal Viscount William Slim described Burma as “some of the world’s worst country, breeding

the world’s worst diseases, and having for half the year at least the world’s worst climate.”² Natural barriers prohibited access to Burma, except by sea and mountain passes. Dense, malarial jungle and impenetrable elephant grass dominated the landscape. Mountain ranges of over 10,000 feet edged the country in a crescent moon, isolating it from India and China. Within Burma, the ranges extended north to south with steep-sided valleys where deep, swift rivers carved their way to swampy deltas and alluvial coastal plains in the south. From June through October, the monsoon season brought heavy rainfall that turned these rivers into torrents and made roads and trails a quagmire.³ Even in the dry season, few passable roads existed, and they and the nation’s limited railways followed the topography’s north-south orientation to converge on the port and capital of Rangoon.⁴ Overall, Burma’s forbidding geography would haunt the Allies as the Japanese commenced their invasion of the country in January 1942.

Following successful campaigns in Malaya and the Dutch East Indies, the Japanese invaded Burma from Thailand. Winning successive battles at Moulmein and the Sittang Bridge, they advanced swiftly to siege Rangoon.⁵ The capital fell in early March, initiating the longest retreat in Britain's military history.⁶ With reinforcements and materiel flowing in through the port at Rangoon, the Japanese offensive steadily gained momentum. The combination of rugged terrain, narrow egress routes packed with refugees, and the Japanese tactic of outflanking and establishing rear-sector roadblocks disrupted the Allies' capacity to feed, supply, and maneuver their forces.⁷ Despite Chinese reinforcements and attempts at a counteroffensive, the Allied retreat continued. Toungoo, Mandalay, Myitkyina, and Akyab fell in rapid succession.⁸ By the end of May, the exhausted, emaciated, and defeated Allied forces reached sanctuary in India when monsoon rains finally halted the Japanese advance.⁹ In 4 months of campaigning, the Japanese had completed their conquest of Burma.

Spurred to raise morale and satisfy political pressures, the Allies launched the first Arakan operation in December 1942.¹⁰ Traversing rugged terrain in a narrow front—"like fighting a modern war along stone-age tracks"—the Allied advance made initial successes before stalling at formidable Japanese bunker complexes.¹¹ Repeated Allied assaults led only to heavy casualties. In April, a Japanese counteroffensive outflanked the Allied positions, and their collapse over the next month was, as Slim wrote, "too much like 1942 over again."¹² The Allies once more retreated to their Indian sanctuary in embarrassing failure as the monsoon rains fell.¹³ As this lamentable scene in the Arakan ended, however, a glimmer of hope materialized with the first Chindit operation.

The Chindits, a diverse force involving British, Gurkha, Burmese, and African units, had spent the previous 3 months penetrating 200 miles into Japanese-occupied Burma.¹⁴ Supplied only by air—their commander Brigadier General Orde Wingate had articulated,

"The vulnerable artery is the line of communication winding through the jungle . . . [to] bring in the goods, like Father Christmas, down the chimney"—the long-range penetration group (LRPG) snaked its way through Burma's treacherous topography, harassing Japanese rear areas and communications.¹⁵ The Chindits successfully cut the Mandalay-Myitkyina railway before attempting to cross the Irrawaddy River to sever the Mandalay-Lashio railway. The combination of exhaustion, disease, overextended air supply, and Japanese attacks forced Wingate to abandon this objective and exfiltrate back to India. Losses were heavy: a third of the force failed to return, and with no means of extracting the wounded, many were left in the jungle to die or be captured.¹⁶ The operation was controversial, delivering no tangible military gains in return for the losses suffered. Yet the audacity and endurance of the Chindits, meeting the Japanese in jungle warfare deep inside their lines, was perceived as a moral victory that inspired Allied forces in India and distracted from the failures in Arakan.¹⁷

For the rest of the 1943 monsoon season, the Allies redressed deficiencies. The command structure reorganized under the newly formed South East Asian Command, appointing Slim as commander of the new XIV Army deployed along a 700-mile front from China to the Bay of Bengal.¹⁸ Changes in command led to a reorientation of strategic, operational, and tactical thinking. Profiting from experience, training expanded to reinforce jungle warfare and mobility, exchanging heavy equipment and motor transport for mule and foot.¹⁹ An offensive mindset ran paramount: Slim emphasized that isolated units would not retreat but stand fast, relying on air supply for sustainment.²⁰ Slim recounted, "We planned the whole of our strategy of this campaign on air supply. There was no main operational plan made in the XIV Army which was not based on air supply."²¹ With the monsoons easing, the Allies showed confidence they had confronted the problems that plagued their earlier defeats and enacted their plan for the reconquest of Burma.

The Second Arakan Operation. In January 1944, the Allied forces commenced their second operation into Arakan, seeking to seize the Maungdaw-Buthidaung Road and destroy the Golden Fortress, a seemingly impregnable web of fortified, interlocking Japanese bunkers and tunnels. Met with fierce resistance, the Allied advance stalled.²² The Japanese opened their counteroffensive in early February, and its speed and magnitude surprised the Allies.²³ Slashing into the rear and then surrounding the 7th Indian Division, the Japanese anticipated a large-scale Allied retreat. Instead, the 7th Indian Division entrenched within the "Admin Box," a 1,200-yard-square semi-fortified position named for a mishmash of buildings, fuel dumps, and arsenals serving as corps headquarters.²⁴

For the next 18 days, the battle ebbed and flowed. Despite ferocious hand-to-hand fighting and raining artillery fire, the Japanese could make no impression against the stubborn Allied defense.²⁵ Although the defenders were supplied with only 2 days' rations when the Japanese attacked, the flat, open ground proved perfect for air supply. C-47 Dakotas braved intense antiaircraft fire for a total of 714 sorties, dropping 2,300 tons of critical relief supplies.²⁶ Allied veterans of the battle would recall, "We only managed because the [Royal Air Force] and Yanks came with their transport planes and dropped ammo to us on parachutes. Barrels of rum, and grub too—same old bully and beans, but it was more than the Japs had."²⁷ Ironically, starvation loomed for the attackers, supplied with only 10 days of rations. The arrival of Allied reserves struck the victorious blow, and the Japanese withdrew, with 5,000 of their original 8,000 dead.²⁸

With the Japanese decisively defeated, the Allied forces regrouped and advanced on their original objectives. By May, the Allies had captured the Golden Fortress and secured an unequivocal victory.²⁹ The second Arakan operation, as Slim declared, "was not of great magnitude, but it was, nevertheless . . . the turning-point of the Burma campaign."³⁰

The Second Chindit Operation. The second Chindit operation commenced concurrently with the series of battles in

Arakan. Codenamed Operation *Thursday* and the brainchild of Wingate, the plan aimed to infiltrate more than 150 miles behind enemy lines to support Allied operations on the Ledo Road, interdict Japanese supply lines, and damage their defenses in northern Burma.³¹ At Wingate's disposal were the equivalent of two divisions of LRPGs, trained explicitly for austere jungle warfare from experiences garnered during the first Chindit operation, and the No. 1 Air Commando Group, a specially trained U.S. Army Air Forces unit of 500 aircraft including supply planes, troop carriers, towed gliders, bombers, helicopters, and fighters. In early February, a single brigade began its trek across challenging terrain into Burma. On March 5, 1944, the main assault began—not by ground but by air, ferried by glider.³²

That night, an armada of C-47s with gliders in tow launched from the airfield at Hailakandi to two landing areas, code-named Broadway and Choringhee. The Chindits experienced no Japanese opposition and secured both landing areas by morning.³³ In the next 6 days, 579 C-47 sorties landed, offloading 9,000 men, 1,300 animals, and 250 tons of stores without loss.³⁴ Wingate now had 12,000 men “inserted in the enemy's guts,” and the operation proceeded toward its objectives.³⁵

Overall, the second Chindit operation proved as controversial as the first. On March 24, Wingate died in a plane crash en route to Imphal, leaving a vacuum of leadership and vision. Subordinated under General Joseph Stilwell, the Chindits spent the following months attempting to capture impregnable Japanese defenses until they were evacuated on the verge of collapse in July. Casualties had soared, and no vital objectives had been met. Though an epic of courage and endurance, the operation became irrelevant to the decisive battles around Imphal and Kohima.³⁶

The Battle of Imphal-Kohima. In early March 1944, the Japanese launched a large-scale offensive into India. By March 29, the Japanese thrust had swiftly surrounded the 150,000-member IV Corps near Imphal and Kohima, severing overland routes for reinforcement or

supply.³⁷ The difference between success and failure depended on air supply.

The Allies anchored their defenses on the 600-square-mile Imphal plain around six airstrips.³⁸ Granted his urgent appeal to divert air transports flying “the Hump”—the trans-Himalaya air supply route from India to China—Slim began the process of reinforcing IV Corps. Within 3 weeks, and 758 sorties later, the entire 5th Indian Division had flown in to bolster defenses.³⁹ With the direct Japanese blow parried, Slim now shifted attention to the supply of Imphal-Kohima.

Aptly named Operation *Stamina*, the air campaign delivered 540 tons of supplies to IV Corps per day.⁴⁰ Over the next 3 months, 404 C-47s transported more than 14 million pounds of rations, 835,000 gallons of fuel, 2.6 million pounds of grain for the pack animals, 12,000 bags of mail, and 43 million cigarettes to the beleaguered Allies.⁴¹ Concurrently, the transports airlifted more than 42,000 noncombatants and 13,000 casualties.⁴² As a result, air supply turned the grim battle of attrition in favor of the Allies.

The fighting around Imphal and Kohima had devolved into a rerun of the Western Front during World War I. Both sides dug in behind bunkers and trenches and fought for every knoll, ridge, and hill.⁴³ Foreseeing a quick rout, the Japanese had commenced their offensive with only 20 days of supplies. With resupply and reinforcement nonexistent, they survived by hunting or capturing Allied airdrops, and the return of the torrential monsoon rains compounded their misery. By July, the ill-equipped and starving Japanese force withdrew across the Burma border in defeat.⁴⁴

The battle of Imphal-Kohima proved an Allied tour de force. Of the 84,000 Japanese who began their offensive, 53,000 became casualties; in contrast, the Allies lost 24,000.⁴⁵ Admiral Lord Louis Mountbatten, the South East Asian Command Supreme Commander, would write, “It is the most important defeat the Japs have ever suffered in their military career.”⁴⁶ As the monsoon rains subsided, the Allies launched their own offensive to finish the war in Burma.

To Rangoon. The great thrust, code-named Operation *Extended Capital*, began in January 1945. Now refitted with mechanized transports and armor, XIV Army slashed its way across the Shwebo Plain of central Burma. With the Japanese entrenched in and around the city of Mandalay, the Allies made a secret dash for Meiktila, the “beating heart” of the Japanese supply effort in Burma and the gateway to Rangoon.⁴⁷

The Allies advanced 200 miles in 20 days, constructing airfields at 50-mile intervals to land supplies and evacuate wounded.⁴⁸ Slim hid his true objective of Meiktila from the Japanese through elaborate deceptions, and he detached a diversionary force to Mandalay to fix the Japanese in place. Convinced by the ruse, the Japanese withdrew forces from the other Burma fronts to reinforce their positions around Mandalay. By the end of February, XIV Army had crossed the Irrawaddy River and clandestinely encircled the Japanese.⁴⁹

Meiktila fell in 4 days, and the Japanese immediately launched a counteroffensive to retake it by siege. Allied reinforcements, however, arrived by air transport to deflect the attack. With the Japanese distracted at Meiktila, Slim ordered the advance on Mandalay. A fierce siege commenced, and the Japanese capitulated on March 20, 1945. Subsequently, the Japanese ceased their attack on Meiktila and withdrew south.⁵⁰ All eyes were now on Rangoon. Slim had only 30 days before the monsoon rains fell and 300 miles to traverse—speed was of the essence.⁵¹

Sprinting across the countryside as a blitzkrieg, XIV Army surged south. The closer it came to Rangoon, the more important was air supply: air transport provided 90 percent of XIV Army's supplies by April.⁵² Slim's rapid success placed a significant stress on air supply, and payloads decreased with each additional mile as cargo weight was traded for fuel.⁵³ Fortunately, a separate Allied offensive on the Arakan peninsula paralleled Slim's advance into central Burma. By February, the Allies had conquered the peninsula and its offshore islands via land and amphibious assaults. By the end of



Bombs cascade from bomb bay doors of B-29 Superfortresses during raid on Japanese supply depots near Mingaladon Airfield, February 28, 1945 (U.S. Army Signal Corps/Library of Congress)

March, they had completed the construction of airfields that brought Rangoon within easy range.⁵⁴

Early monsoon rains, however, beset XIV Army's lunge south. The possibility of conducting a siege in these conditions led Slim to accept Operation *Dracula*.⁵⁵ On May 1, an 800-member brigade parachuted into the outskirts of Rangoon, clearing the approach for an amphibious assault that occupied the city the following day. There was no resistance; the Japanese had already evacuated.⁵⁶ Overwhelmed by torrential downpours, XIV Army halted 41 miles from Rangoon that same day.⁵⁷ The campaign to reconquer Burma had come to an anticlimactic yet triumphant conclusion.

Inferences for Joint Force Operations in the Indo-Pacific Region

Allied and Japanese experiences during the 1942–1945 Burma campaign are rich in data from which to draw infer-

ences for future joint force operations in the Indo-Pacific region. The 80-year time span since those events qualifies the premises drawn from them: the character of warfare and its technology have changed. Air mobility and aerial resupply methods, emergent during the Burma campaign, continue as standard practices among all modern militaries. Long-range insertion and resupply of special operations forces (SOF), also pioneered during this campaign, are available to any military with the right troops, aircraft, and training.

Since the early innovations of Burma, the technologies to perform these methods of war are far more advanced, as are the countermeasures to oppose them. Transport aircraft have longer ranges and payloads than C-47 Dakotas and C-46 Commandos. Supplies can be airdropped in large quantities and with high precision. Modern rotary and tilt-rotor aircraft provide vertical air transport options. Unlike Wingate's Chindits, modern

special operations units are purpose-built and equipped to fight and survive in harsh environments. Conversely, the integrated air defenses that characterize advanced threat environments are deadly to aircraft and any troops they transport. Sensor networks that cue these defenses can easily detect all but stealth assets, and large ground formations are difficult to conceal. The means to destroy these forces once detected are orders of magnitude more rapid, precise, and lethal than in the 1940s. The Burma campaign differs markedly from modern campaigning in that the former relied explicitly on air mobility and the air supply of troops, whereas the latter must exist in advanced threat environments where the ability to perform these functions is highly contested.

Even with these caveats, the relevance of the Burma experience and its insights for modern joint force operations are striking. Though in a different adversarial configuration, the primary belligerents in Burma—the United States, United

Kingdom, China, and Japan—would likely face each other in a significant conflict in the Indo-Pacific and indeed are engaged in competition today. The Burma campaign occurred near China's border; a contemporary conflict in this same theater is plausible, and the physical terrain is virtually unchanged. The balancing effects of Allied mass versus Japanese proficiency seen in Burma might be reversed in a modern Indo-Pacific conflict, where U.S. warfighting proficiency would meet the mass of China's People's Liberation Army. The force-multiplier effect of partner forces, from international allies to local tribes, was crucial then, and it remains so. The functions of maneuver and resupply remain no less decisive, though the threats that oppose them are more intense.

One solution to a contested air environment is to fight for local air superiority at the time and place of necessity. In 1942, Japan had air superiority in

Burma. By 1943, however, the Allies had regained this advantage, and it proved critical at Imphal-Kohima.⁵⁸ Slim's XIV Army capitalized on its ability to move troops and supplies in and casualties out, sustaining its forces to outlast a determined Japanese assault.⁵⁹ In a contemporary conflict in the Indo-Pacific, the United States and its allies would be likely to operate in a persistently contested air environment. Air supremacy across the theater is unrealistic. Joint forces would need to fight for air superiority when and where needed and exploit temporary and local advantages.

Another solution to contested air is to fight through it despite the risk. During the second Arakan operation, Japanese antiaircraft fire and fighter opposition around the Admin Box proved so intense that resupply aircraft turned back. Brigadier General William Old rallied his airmen by personally flying an

aircraft to supply the Box.⁶⁰ Where air superiority cannot be achieved today, the joint force may employ remotely piloted, autonomous, and "attritable" aircraft to maneuver and supply ground troops. In cases where manned aircraft must be used and military necessity outweighs risk, the joint force must be prepared to face and recover from painful losses.

The Japanese army masterfully employed a simple countermeasure when facing overwhelming air superiority: they dug. Their underground bunkers and tunnels at Kohima withstood direct hits from artillery and fighter-bombers. Japanese infantry had to be blasted out of their bunkers at close range by tanks or buried alive when tanks drove over them.⁶¹ Simplistic as it may appear, modern joint forces can survive by digging in against superior firepower, including modern precision and standoff fires, and can expect adversaries to do the same.



Chindits commander General Orde Wingate (wearing pith helmet) briefs members of 1st Air Commando, U.S. Army Air Force, in Burma, circa 1944 (PA Images/Alamy)

Moreover, many operations in Burma depended on physical stamina. Despite the prevalence of airpower, artillery, and heavy weapons, battles were often fought in hand-to-hand combat with swords and bayonets.⁶² Wingate's Chindits trained for months to patrol on foot at great distances, requiring extraordinary physical endurance.⁶³ Clearing Japanese bunkers around Imphal-Kohima relied on bayonet attacks as much as tanks.⁶⁴ Advanced technology cannot replace, but must complement, courage and physical strength at the individual level, with implications for joint force training and readiness.

Though the Chindit operations met with mixed tactical success, they presented operational dilemmas that forced the Japanese to contend with formations deep inside their lines. The joint force can employ special operations to similarly "expand the competitive space" in competition and achieve strategic surprise in conflict. Conventional forces operating at standoff ranges are likely to rely on SOF to stand in to perform functions including reconnaissance, terminal guidance, and battle damage assessments. Like the Chindits, they will need mobility and sustainment to bring supplies in and casualties out. The joint force must improve existing capabilities to maneuver small teams and supply them at long range, inside the weapons engagement zones of advanced threats. Noting the importance of river crossings and the use of frogmen and a special boat unit to reconnoiter the far bank of the Irrawaddy, future campaigns in the Indo-Pacific region will require undersea, surface, and riverine mobility to move and supply special operations and other stand-in forces in the littorals and inland waterways.⁶⁵

Implications for Future Operational Design

Beyond the tactical, readiness, and capability inferences drawn from Burma, there are significant implications for joint force operational design. First, the Burma campaign involved asymmetries of firepower on the Allied side and proficiency on the Japanese side, which could counterbalance each

other depending on degrees of advantage and contextual factors. Second, the Allies' use of diverse forces and capabilities proved an advantage against a homogeneous and cohesive adversary. Third, although they sometimes plodded at the tactical level, the Allies were agile and creative in the art of campaigning. Finally, successful maneuver and sustainment were decisive to the Allied campaign.

The superior proficiency of the Japanese infantry was remarkable. During the first Arakan campaign, the Allies had control of the skies, superior firepower, and numerical superiority. The Japanese, nevertheless, used carefully constructed bunkers to halt their advance and outmaneuvered Allied forces with infiltration tactics, night attacks, and jungle warfare.⁶⁶ The Allied victory in the second Arakan operation dispelled the myth of Japanese invincibility, but the fact of Japan's infantry advantage remained. At Imphal-Kohima, Japanese forces surrounded XIV Army and held on for 4 months in the face of overwhelming firepower despite debilitating infighting among senior commanders.⁶⁷ Acknowledging this asymmetry, Slim urged his superiors to improve the proficiency of British forces and the Allies. Wingate's Bush Warfare School took a step in this direction by training the Chindits to be physically tough and tactically proficient in jungle warfare.⁶⁸ Given the pace at which the People's Republic of China has modernized and built up its forces, the joint force and its allies cannot rely on superior firepower, mass, or qualitative technological advantages. To account for this situation, operational design should endeavor to widen advantages in proficiency and leadership to neutralize opponent strengths in mass and technology.

Furthermore, the Allied force in Burma consisted of British, Indian, Burmese, American, Chinese, and other forces, including local tribal partners. Although the Japanese founded the Indian National Army and Burmese National Army, their accomplishments were limited.⁶⁹ In contrast, XIV Army leveraged the diversity within its force

and built partnerships with local tribes.⁷⁰ Similarly, the joint force of today is increasingly diverse. U.S. alliances and partnerships offer comparative advantages that authoritarian competitors cannot approach. Future operational designs should build on these relationships and leverage them as a qualitative edge for competition and campaigning in the Indo-Pacific region.

Joint force operational design should also emulate the Allies' superior use of operational art in Burma. The Japanese fought well but hardly campaigned. Rather, they sought to aggregate small victories into large ones and repeated standard tactics even when those tactics stopped working. Their leadership at the operational level was feckless and failed to adapt to the changing conditions of battle.⁷¹ In contrast, the Allies overcame comparative disadvantages in training and proficiency with superior operational art. Innovations in air resupply, air mobility, and commando raiding followed from the creativity and adaptability of Mountbatten, Slim, and Wingate. If contemporary joint force commanders and staffs practice equally inspired operational art, emergent designs could prove decisive to competition and campaigning.

The Allies' innovative use of operational maneuver was critical to their success in Burma and is equally critical to contemporary operational design. In Operation *Thursday*, the Chindits maneuvered above and penetrated well inside Japanese lines through the air domain, revealing the offensive potential of the Allies and instigating the disastrous Japanese assault on Imphal-Kohima.⁷² The blitzkrieg tactics of XIV Army in Operation *Extended Capital*, sweeping southward through central Burma toward Rangoon, denied the enemy options in time and space and exploited Japanese vulnerabilities at the operational level. Future operational designs in the Indo-Pacific can reprise these approaches. Future battlefields will contest theater access and maneuver. Operational design must incorporate new methods and technologies that remove barriers and facilitate actions through multiple domains simultaneously. Maneuvers executed



British infantrymen fire mortar bombs during Battle of Imphal in region around city of Imphal, in Northeast India, circa March–July 1944 (De Luan/Alamy)

with simultaneity and depth through cross-domain operations will dislocate the enemy and outpace its capacity to respond. Future operational designs can control the initiative by incorporating creative schemes of maneuver that sustain momentum throughout the operation, exploiting comparative temporal advantages that deny the enemy options.

Arguably, the Burma campaign was the singular World War II operation that required, not merely benefited from, sustainment and its capacity to alter the geometry of the battlefield. The historian David W. Hogan, Jr., notes, “The [Burma] theater lay at the end of long lines of communications extending halfway around the world from Britain to the United States. That, and strategic priorities, resulted in shortages of nearly every item of supply.”⁷³ Slim’s ability to extend the operational reach of XIV Army through air supply represented a strategic shift that nullified Japanese tactical advantages. Absent their innovations in logistics and sustainment by air,

the Chindit operations would never have launched, the second Arakan operation would have echoed the disasters of the first, Imphal-Kohima would have fallen to the Japanese, and the march to Rangoon would have stalled in quagmire.⁷⁴ Future operational designs must place sustainment at the forefront of their concepts and methods. Joint force planners must envision sustainment as the lead enabler for strategic, operational, and tactical reach in the long-range battlefields of the Indo-Pacific. If future operational designs postulate unrealistic and unsustainable approaches, they will not succeed in leveraging the full warfighting potential of the joint force.

Conclusion

The Burma campaign was a series of reversals in fortune. The Japanese triumph in 1942 devolved into the most significant defeat in Japanese army history in 1945, and the British tragedy of 1942 evolved into the decisive victory in 1945. The campaign was

also a war of extremes. The belligerents operated in a theater as remote from Japan as from Britain. Battles were waged in impenetrable jungles, on steep mountainsides, and across raging rivers and scorching alluvial plains. Hand-to-hand combat existed alongside the airlift of whole divisions. Gliders inserted LRPGs into Burma’s jungles while soldiers marched through sheets of monsoon rain. Trench warfare gave way to blitzkrieg.

Although the details of the longest campaign of World War II are historically unique, the inferences gained concerning the relationships among technology, readiness, and operational and tactical capabilities are relevant today. The Burma experience reaffirms the aphorism that local air superiority is a prerequisite for any modern joint force operation. Despite the risk inherent in operating on future battlefields, joint force commanders and their staffs must acknowledge and recover from realistic and painful losses. As in Burma then and

in the Indo-Pacific today, innovations in technology and methods can deliver qualitative advantages. One solution for survivability is subterranean defenses against superior firepower. Another is presenting operational dilemmas to the enemy that “expand the competitive space.” Furthermore, morale and physical elements proved critical in delivering an Allied victory in Burma. Modern technology cannot substitute for, but must supplement, courage and physical strength at the individual level.

These inferences drawn from the Burma campaign can lead to significant implications for joint force operational design. The asymmetries of Allied firepower vis-à-vis Japanese proficiency counterbalanced each other throughout the campaign. The rate at which the People’s Republic of China has modernized its military dictates that the joint force cannot solely rely on superior firepower as a comparative advantage. Operational design should account for this aspect and seek to widen U.S. advantages in proficiency and leadership. Moreover, the diverse makeup of the Allied force in Burma delivered an advantage unavailable to a homogeneous adversary. Future operational designs should build on the joint force’s relationships with allies and like-minded partners, leveraging them as a qualitative edge in the Indo-Pacific region. Joint force operational design should also emulate the Allies’ superior use of operational art in Burma. Finally, the Burma campaign demonstrated the comparative advantage gained by maneuver and sustainment. The Allies’ ability to combine strategic and operational ends with logistical means determined tactical, operational, and strategic effectiveness. Future joint force operational designs must seize the initiative through timely maneuvers in multiple domains. These designs must also prioritize sustainment as a vital function to negate the tyranny of distance inherent in the Indo-Pacific theater. Ultimately, the Burma campaign of World War II provided a kaleidoscope of inferences for the contemporary joint force that color implications for future operational designs in the Indo-Pacific. JFQ

Notes

- ¹ Louis Allen, *Burma: The Longest War, 1941–45* (London: Phoenix Press, 2000), xvii–xx.
- ² Viscount William Slim, *Defeat Into Victory: Battling Japan in Burma and India, 1942–1945* (New York: Cooper Square Press, 2000), 169.
- ³ Joe G. Taylor, *Air Supply in the Burma Campaigns*, USAF Historical Studies No. 75 (Maxwell AFB, AL: Research Studies Institute, 1957), 1–3, available at <https://apps.dtic.mil/sti/pdfs/ADA529960.pdf>.
- ⁴ David Rooney, *Burma Victory: Imphal, Kohima, and the Chindits, March 1944 to May 1945* (London: Osprey Publishing, 2014), 13.
- ⁵ Raymond Callahan, *Burma, 1942–1945: The Politics and Strategy of the Second World War* (Newark: University of Delaware Press, 1979), 34–36.
- ⁶ Richard Holmes, ed., *The Oxford Companion to Military History* (Oxford: Oxford University Press, 2001), 160.
- ⁷ Slim, *Defeat Into Victory*, 29; Frank McLynn, *The Burma Campaign: Disaster Into Triumph, 1942–45* (New Haven: Yale University Press, 2011), 109.
- ⁸ Taylor, *Air Supply in the Burma Campaigns*, 4.
- ⁹ Slim, *Defeat Into Victory*, 111–112.
- ¹⁰ McLynn, *The Burma Campaign*, 98.
- ¹¹ Allen, *Burma*, 97; Slim, *Defeat Into Victory*, 100–101.
- ¹² Slim, *Defeat Into Victory*, 160.
- ¹³ Callahan, *Burma*, 62–63.
- ¹⁴ McLynn, *The Burma Campaign*, 88; Slim, *Defeat Into Victory*, 162.
- ¹⁵ Colin Higgs, *Wingate’s Men: The Chindit Operations: Special Forces in Burma* (Barnsley, Yorkshire, UK: Frontline Books, 2019), 4.
- ¹⁶ Allen, *Burma*, 123, 143.
- ¹⁷ Slim, *Defeat Into Victory*, 162; Callahan, *Burma*, 66–67.
- ¹⁸ McLynn, *The Burma Campaign*, 189, 209.
- ¹⁹ Callahan, *Burma*, 98.
- ²⁰ *Ibid.*, 132.
- ²¹ Gerald Astor, *The Jungle War: Mavericks, Marauders, and Madmen in the China-Burma-India Theater of World War II* (Hoboken, NJ: J. Wiley & Sons, 2004), 6.
- ²² McLynn, *The Burma Campaign*, 250–252.
- ²³ Slim, *Defeat Into Victory*, 235.
- ²⁴ Allen, *Burma*, 182–186.
- ²⁵ McLynn, *The Burma Campaign*, 253.
- ²⁶ Roger Annett, *Drop Zone Burma: Adventures in Allied Air-Supply, 1943–45* (Barnsley, Yorkshire, UK: Pen & Sword Aviation, 2008), 81; S. Woodburn Kirby, *The War Against Japan*, vol. 3, *The Decisive Battles* (Uckfield, East Sussex, UK: Naval & Military Press, Ltd., 1961; rpt. 2004), 144.
- ²⁷ Annett, *Drop Zone Burma*, 81.
- ²⁸ McLynn, *The Burma Campaign*, 254.
- ²⁹ *Ibid.*, 255.
- ³⁰ Slim, *Defeat Into Victory*, 246.

- ³¹ McLynn, *The Burma Campaign*, 275.
- ³² Lowell Thomas, *Back to Mandalay* (London: F. Muller, 1962), 14–19.
- ³³ McLynn, *The Burma Campaign*, 281.
- ³⁴ Shelford Bidwell, *The Chindit War: Stilwell, Wingate, and the Campaign in Burma, 1944* (New York: Macmillan, 1980), 110.
- ³⁵ McLynn, *The Burma Campaign*, 283.
- ³⁶ Callahan, *Burma*, 138–139.
- ³⁷ Allen, *Burma*, 244.
- ³⁸ Slim, *Defeat Into Victory*, 293.
- ³⁹ Norman Franks, *The Air Battle of Imphal* (London: Kimber, 1985), 37.
- ⁴⁰ Allen, *Burma*, 244.
- ⁴¹ Geoffrey Evans and Antony Brett-James, *Imphal: A Flower on Lofty Heights* (London: Macmillan, 1962), 204.
- ⁴² Allen, *Burma*, 244.
- ⁴³ McLynn, *The Burma Campaign*, 307.
- ⁴⁴ *Ibid.*, 326.
- ⁴⁵ Callahan, *Burma*, 137; McLynn, *The Burma Campaign*, 323.
- ⁴⁶ McLynn, *The Burma Campaign*, 323.
- ⁴⁷ *Ibid.*, 415.
- ⁴⁸ S. Woodburn Kirby, *The War Against Japan*, vol. IV, *The Reconquest of Burma* (London: Her Majesty’s Stationery Office, 1965), 186; Allen, *Burma*, 403–405.
- ⁴⁹ Slim, *Defeat Into Victory*, 393, 436; Callahan, *Burma*, 157–158.
- ⁵⁰ Slim, *Defeat Into Victory*, 454; Callahan, *Burma*, 157–159; McLynn, *The Burma Campaign*, 159.
- ⁵¹ Ronald Lewin, *Slim: The Standardbearer* (London: Cooper, 1976), 232–233.
- ⁵² *Ibid.*, 217; Robert Lyman, *Slim, Master of War: Burma and the Birth of Modern Warfare* (London: Constable, 2004), 248.
- ⁵³ United Kingdom Air Ministry, *Wings of the Phoenix: The Official Story of the Air War in Burma* (London: Her Majesty’s Stationery Office, 1949), 118.
- ⁵⁴ Slim, *Defeat Into Victory*, 458–464; Callahan, *Burma*, 159.
- ⁵⁵ Slim, *Defeat Into Victory*, 481.
- ⁵⁶ McLynn, *The Burma Campaign*, 443.
- ⁵⁷ Callahan, *Burma*, 160.
- ⁵⁸ Allen, *Burma*, 154.
- ⁵⁹ *Ibid.*, 242–244.
- ⁶⁰ *Ibid.*, 187.
- ⁶¹ *Ibid.*, 257, 272.
- ⁶² *Ibid.*, 215.
- ⁶³ *Ibid.*, 123.
- ⁶⁴ *Ibid.*, 257–258.
- ⁶⁵ *Ibid.*, 417.
- ⁶⁶ *Ibid.*, 97–98.
- ⁶⁷ *Ibid.*, 307–308.
- ⁶⁸ *Ibid.*, 114, 123.
- ⁶⁹ *Ibid.*, 226–227.
- ⁷⁰ *Ibid.*, 147, 213, 230.
- ⁷¹ *Ibid.*, 297.
- ⁷² *Ibid.*, 150.
- ⁷³ Slim, *Defeat Into Victory*, x.
- ⁷⁴ Taylor, *Air Supply in the Burma Campaigns*, 148.



Leadership Decapitation: Strategic Targeting of Terrorist Organizations

By Jenna Jordan

Stanford University Press, 2019

272 pp. \$39.95

ISBN: 9781503608245

Reviewed by Larry D. Miller

Leadership decapitation has become increasingly popular as an efficient, economical, and effective counterterrorism option for advancing U.S. interests when dealing with organizations willing to kill civilians in pursuit of political ends. But does the removal of violent nonstate leaders actually yield demonstrably favorable results beyond the obvious: execution or apprehension of a target? Does it, in fact, weaken or bring about the demise of terrorist organizations? In *Leadership Decapitation: Strategic Targeting of Terrorist Organizations*, Jenna Jordan addresses such questions by offering a complex and nuanced discussion of the ways that leadership decapitation affects terrorist organizations and insurgencies that kill civilians.

Ineffective leadership decapitation is that which does not weaken or

meaningfully diminish the operational capacity of the decapitated organization. Through analysis and evidence-based argument, Jordan convincingly demonstrates that “leadership targeting has been largely ineffective” in weakening and destabilizing terrorist organizations and often results in increased radicalization and terrorism. Jordan acknowledges, nevertheless, that leadership decapitation is likely to remain a viable policy option—albeit an option largely absent evidence-based guidance for predicting outcomes, until now. Jordan’s analysis and research indicate that anticipating, indeed predicting, outcomes following decapitation is possible. Her detailed research report warrants judicious consideration by senior government and military officials who recommend decapitations and those who authorize them.

Jordan offers the context, theory, data, extensive statistical analyses, and multiple case studies necessary to understand (1) if and when eliminating high-value terrorist leaders reduces terrorism and weakens terrorist organizations, (2) under what circumstances decapitation is unlikely to produce the result intended, and (3) which variables warrant judicious consideration when decapitation is both feasible and consistent with policy goals. The book opens with a well-crafted introduction that defines essential terms, presents her argument and method, summarizes decapitation research, and acknowledges the limitations of leadership decapitation. Following a crisp review of relevant leadership literature, Jordan persuasively argues that organizational resilience accounts for and predicts the impact of decapitation.

Resilient terrorist organizations—though they may be shocked, angered, or inconvenienced by the loss of a leader—do not make good targets for leadership decapitation if the goal is to reduce future threats and weaken the organization. As Jordan explains, resilient organizations benefit from a bureaucratic structure that maintains normative rules and expectations, communal support, and access to essential resources (money, recruits, information, intelligence, and security). Resilient organizations also

tend to have a strong anchoring ideology or belief structure that is endemic among adherents and peripheral supporters.

Jordan advances this theory of organizational resilience as a way to account for variations in organizational response once the leader has been eliminated through death or capture.

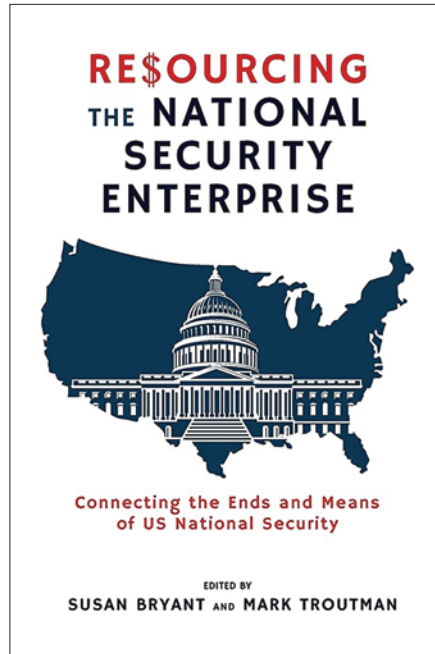
To assess relevant hypotheses, Jordan assembled a database of 1,276 instances of leadership targeting that occurred worldwide between 1970 and 2016. Among the findings: (1) the successful removal of top leadership generates a greater reduction in terrorist activity than does the elimination of the upper echelon of leadership; (2) within the first year following decapitation, Islamist groups are nearly three (2.87) times more likely than non-Islamist groups to renew terrorist attacks; (3) Islamist groups targeted for decapitation are “more likely to increase [terrorist] activity than non-decapitated groups”; and (4) on balance the data indicate that whereas decapitation sometimes works as a counterterrorism tool, it is unlikely to have much effect “against organizations such as ISIS, al Qaeda, and Hamas.”

Jordan presents three highly informative, readable, and detailed case studies of organizations that use terror for political ends: Hamas, the Shining Path, and al Qaeda. Each case study demonstrates the utility of her application of organizational resilience theory to leadership targeting and decapitation. The Hamas case study (chapter 5) explores how its leadership has survived 81 targeting incidents and how a well-structured bureaucracy, delivery of social services, and community support insulate Hamas from organizational demise following leadership decapitation. The Shining Path case study (chapter 6) explores the ways that group dynamics contributed to the demise of the left-wing Peruvian communist insurgency. Although two of the Shining Path’s leaders (Abimael Guzman and, later, Oscar Durand) were forcibly removed, Jordan maintains that the demise of the Shining Path can be traced to bureaucratic deficiencies and the attendant loss of community support rather than primarily to leadership decapitation. The al

Qaeda case study (chapter 7) is primarily a consideration of religious ideology and organizational resilience. Following the death of Osama bin Laden, predictions were rampant that his death foreshadowed the end of al Qaeda's operational capability. In part, that expectation never materialized because, Jordan argues, al Qaeda morphed into a meta-organization operating through autonomous groups bound by a common ideology and shared goals. Thus, al Qaeda is not a single unified terrorist organization but, rather, a system of loose affiliates each with functional bureaucracies, communal support, and deep adherence to Islamist principles and teachings.

Leadership Decapitation is as challenging as it is informative. The book is comprehensively packed, highly detailed, and supported by multivariate analyses, transition matrices, time series analyses, extensive chapter notes, and a substantial bibliography. Jordan's book will appeal to two modestly overlapping audiences: data analysts and quantitative researchers who study terror, and senior defense officials and joint force leaders who necessarily deal with it in the real world. Scholars and others familiar with sophisticated statistical modeling and analyses will find the work stimulating, insightful, and informative; yet, generally, that audience lacks the authority to shape counterterrorism policy and/or target terrorist leaders. Conversely, those who shape policy and are positioned to authorize lethal decisions may be skeptical of numerical data and analyses that appear to fly in the face of common sense and post-9/11 practice. Notwithstanding receptivity and accessibility issues, Jordan's book is an original and valuable contribution to understanding how terrorist organizations and insurgencies survive following the death or capture of senior leadership. JFQ

Larry D. Miller, Ph.D., directs The Inquiry Project for Communication Research, Cable Creek Publishing, and is a Faculty Instructor, Department of Distance Education, at the U.S. Army War College.



Resourcing the National Security Enterprise: Connecting the Ends and Means of U.S. National Security

Edited by Susan Bryant and Mark Troutman
Cambria Press, 2022
279 pp. \$39.99
ISBN: 9781621966241

Reviewed by Stephan Pikner

Books on strategy are often aspirational or theoretical, considering high-level questions, first principles, and general trends without delving deeply into the mechanics of implementation. Similarly, a parallel vein of literature focuses on a narrow range of tactical platforms or concepts in the implicit hope that someone somewhere will use these clever tools to build a future force from the bottom up. *Resourcing the National Security Enterprise: Connecting the Ends and Means of U.S. National Security* fits squarely between these two attractive yet unsatisfying poles; it is a practitioner's guide to programming and budgeting that aims to demystify the "invisible but very real web of processes and authorities [that] constitute the 'rules of the game' for

the bureaucracy"—"rules which often forestall the 'obvious solution'" to government workers' problems.

This edited volume draws on the expertise of 10 highly regarded contributors, all of whom bring deep familiarity with a specific corner of the larger national security enterprise to their chapters. Strongest of these is John Ferrari's chapter on programming strategic priorities, a topic covered in exhaustive, technical detail elsewhere that comes to life through sharp and insightful prose that returns to a common theme: "There are no shortcuts; only by understanding time and bounding the strategy to available resources can a strategist be effective." This is not a passive subordination of strategy to budget constraints: "A strategy can drive resource allocations, but only if it works effectively within the constraints of the decade-long national cycle of funding." *Resourcing the National Security Enterprise* shines brightest when it is outlining these constraints while highlighting where sustained progress can be made.

A discussion of the role of Congress in budget formation by Heidi Demarest opens a series of chapters that touch on different portions of the Federal government. Demarest focuses on congressional staffers, particularly the relative decline in their typical national security expertise since the end of the Cold War. Jason Galui's chapter on the National Security Council centers on the Office of Management and Budget's role in crafting the Presidential budget submission, an effort Galui calls "the structural support of the NSC strategy bridge." Importantly, these chapters (and the volume itself) sidestep personalities and partisanship and instead dive deeply into the mechanics "under the hood" of the programming and budgeting cycle.

In contrast to other works that focus narrowly on the military, *Resourcing the National Security Enterprise* takes a refreshingly broad view, extending beyond the Department of Defense (DOD). Particularly welcome in this regard are contributions by Geoffrey Odium on funding U.S. diplomatic priorities, Rebecca Patterson on resourcing U.S. partners and allies, and Mark Troutman

on the Department of Homeland Security (DHS). Odum offers a candid diagnosis of the bureaucratic and cultural impediments to effective strategic planning and programming in the State Department, which, though “sufficient to muddle through and with diplomatic tools and programs that remain planned and funded well enough to react” to an immediate, local crisis, can end in larger “policy failure [that] is most often the result of poor planning or poorly managed implementation or both.” Patterson highlights the value to the United States of sustained funding for United Nations (UN) peacekeeping operations as an affordable hedge against instability in troubled regions. This argument, carried forward from the political science literature on post-conflict stability and reinforced with a detailed discussion of UN funding pathways and resourcing, is an intriguing direction that merits broader incorporation in discussions of force employment and competing operational demands. Troutman’s chapter is equally illuminating, tracing the evolution of DHS since its founding nearly two decades ago. He diagnoses the fundamental challenge faced by the department clearly: “The DHS is neither a peripheral nor a temporary addition to U.S. national security. However, it is resourced and organized as though it were both.” Of the various thoughtful recommendations for reform and process modernization across the volume, the succinct set of proposals that Troutman ends his chapter with hits the hardest.

Resourcing the National Security Enterprise is at its softest when it bemoans larger trends such as increased nondiscretionary spending, the expanding national debt, and the projected slowing of economic growth. Although these trends do matter, the cursory treatment they receive at several points oversimplifies the uncertainty and complexity in such projections, ignores the sound advice offered elsewhere to acknowledge that some things are beyond a security strategist’s control, and distracts from the overall thrust of the chapter. Left underdeveloped is the argument that many of these same trends—namely,

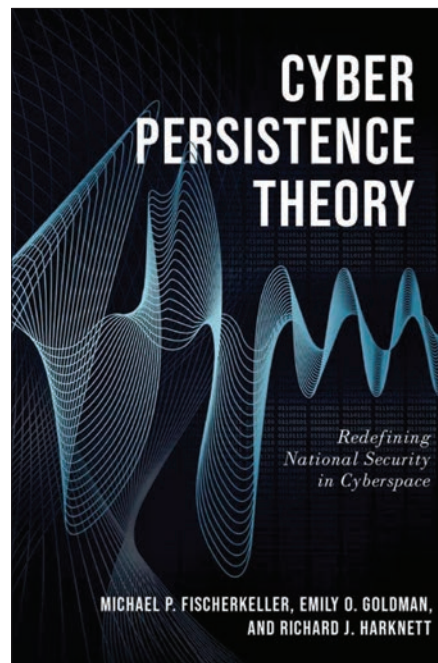
rapidly increasing health care, higher education, housing, and pension costs—detract as much from the proportion of the military’s overall budget spent narrowly on modernization and training as from DOD’s overall relative share of the Nation’s production. More narrowly, the book leaves unexplored the challenges facing the Navy as it balances tradeoffs between fleet size, emerging adversary capabilities, operational tempo, and modernization, all against the backdrop of limited shipyard capacity. The forces that led the sea Service to overinvest in some platforms at the expense of others in prior decades are worthy of separate, deep study, but (at a minimum) a nod to the dynamics driving the Navy’s shipbuilding plans would have made *Resourcing the National Security Enterprise* a richer read.

Those minor critiques aside, a close reading of *Resourcing the National Security Enterprise* is a valuable starting point for the deeper understanding required to guide the fundamental processes that shape our national defense. As Ferrari, a retired Army major general, ends his contribution,

To have true positive influence on the process requires investing hundreds of hours in preparation and working multiple jobs in the Pentagon. High rank and position cannot shortcut the process. Part-time programming may alone account for the dismal outcomes associated with America’s first battles.

This volume has earned a place on strategists’ bookshelves and consideration for inclusion in higher-level professional military education curricula. Perhaps more important, its underlying message, that budgeting and programming experience is both invaluable and irreplaceable, should guide career managers and mentors as they steer promising officers toward assignments of greatest impact. JFQ

Lieutenant Colonel Stephan Pikner (FA59) is the Military Advisor to the Director, Office of the Secretary of Defense, Office of Net Assessment.



Cyber Persistence Theory: Redefining National Security in Cyberspace

By Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett
Oxford University Press, 2022
266 pp. \$28.45
ISBN: 9780197638262

Reviewed by Stafford A. Ward

Few books have been written in the recent past whose stated intent has been to influence and shape the perceptions of foreign and defense policymakers. In the spirit of the famed Stanford University political scientist Alexander George, who wrote *Bridging the Gap: Theory and Policy in Foreign Policy*, the authors of *Cyber Persistence Theory: Redefining National Security in Cyberspace* have successfully bridged the gap with a thought-provoking, accessible academic analysis. *Cyber Persistence Theory* holistically examines the current cyberspace environment in a way that is sure to be useful to U.S. cyberspace policymakers and operators.

The arguments advanced by the writers artfully explore the structure of the new cyberspace environment. The authors are a qualified mix of

cyberspace academics and practitioners who succinctly capture their previously published thoughts on cyberspace to advance a coherent and novel concept of cyber persistence theory. Successfully communicating a theory to a range of communities can be a heavy lift, but the authors have included extensive footnotes that provide resources through which readers can delve deeper as needed into the concepts discussed, such as structural realism, agreed competition, balance of power, and offense-defense theory.

The heart of *Cyber Persistence Theory* explains that

the primary [cyber faits accomplis] and secondary [direct cyber engagement] behaviors of States in and through the cyber strategic environment . . . are consequences of a structural imperative to persist and of a structurally derived strategic incentive to pursue gains through cyber exploitation short of armed-attack equivalence.

This theory argues that cyberspace exploitation, the most dominant form of cyberspace activity, represents strategic competition and therefore should be understood as one state's gaining cyberspace advantage through another's cyberspace vulnerabilities in a short time frame. To make their case, the authors consider various international relations theories and strategic concepts to establish the foundation of persistence theory for the reader. They bridge the gap by drawing on international affairs scholarship by authors including military and nuclear strategists such as Thomas Schelling, Kenneth Waltz, Carl von Clausewitz, and Bernard Brodie, as well as scientific philosopher Thomas Kuhn. In particular, the authors acknowledge Waltz, the founder of neorealism, or structural realism, as defining the international system as a "condition of insecurity . . . that works against [international] cooperation." Because states in our era of Great Power competition are leveraging malicious cyberspace activities as an alternate means of accomplishing their geopolitical goals, there is no inherent incentive for those states to cooperate as they would in the concert of

international diplomacy. In sum, there is no United Nations in cyberspace.

The first four chapters of the book thoroughly explain the theoretical concepts that define the cyberspace environment; they are followed by several chapters examining real-world cases of cyberspace campaigns among both micro-resilient and micro-vulnerable states. For example, the authors highlight the U.S. Government's cyberspace operations to disrupt the so-called Islamic State's online propaganda activities, Russia's compromise of U.S. networks, and China's zero-day exploitations of commonly used software applications, such as Microsoft Exchange and Adobe Flash.

With the foundations of cyber persistence theory established, the authors move to explain the three strategic environments that characterize the entire human history of security: conventional, nuclear, and cyberspace. Conventional security rests in the presence of war, nuclear security rests in the absence of war, and cyber security rests in the alternative to war. The authors point out that most policymakers and operators currently frame cyberspace in a Cold War context, which maps inaccurately to the current strategic cyberspace environment. The authors argue that "interconnectedness" is the core structural feature of the cyber strategic environment, requiring continuous integrated campaigning and supported by ongoing collaboration, integration, and synchronization across all relevant cyber planning and operational players and all instruments of national power. Cyber persistence theory also suggests that cyberspace operations are not inherently escalatory, and such operations rarely cross the upper bound of agreed competition, or the threshold of warfare, into kinetic operations.

Cyber Persistence Theory also defines the evolution from the two strategic environments to the current cyberspace strategic environment as a paradigm shift that necessitates a change in strategic thinking among policymakers, senior defense leaders, and joint force operators. Thomas Kuhn, the authors note, "writes that a paradigm provides a community with its basic assumptions, key concepts, and

methodology. . . . For a shift, or 'change in worldview,' to occur, there must be a realization of the misalignment between theory and reality." The authors argue that the misapplication of the paradigms of conventional and nuclear environments to cyberspace represents a failure to understand the nature of the cyber environment. This is sure to generate discussion among scholars and strategists alike. For example, *Cyber Persistence Theory* argues that cyber policymakers who plan to hold cyber targets at risk fail to understand that cyberspace is an environment where seizing targets of opportunity is a better policy prescription, given the highly dynamic nature of cyberspace.

The authors also offer insights for diplomats and specialists in international law who must devise methods for minimizing risks inherent in the international system due to malicious cyber activities. As supplementary reading, policymakers and joint force operators should consider the late Columbia University political scientist Robert Jervis's essay "Cooperation Under the Security Dilemma," to aid in their addressing international cooperation in cyberspace. Would inter-state cooperation create security advantages among like-minded states in an environment of interconnectedness? Is Waltz correct that such cooperation in cyberspace might not completely provide states with security guarantees against states acting outside of responsible cyberspace norms?

Cyber Persistence Theory will help policymakers and cyberspace warriors and operators to make sense of the work they do daily, offer a sense of purpose, and help to both shape and articulate the cyberspace environment. *Cyberspace Persistence Theory* should be mandatory reading for joint force operators, policymakers, diplomats, and law enforcement specialists, to provide them with a richer understanding of early-21st-century cyberspace. JFQ

Stafford A. Ward is a Cyberspace Integration Planner in the Partnerships Division at U.S. Cyber Command (USCYBERCOM) and is also a USCYBERCOM Commander's Civilian Development Fellow, in a program established by USCYBERCOM Commander General Paul Nakasone.

Falcon 9 rocket carrying Starlink 4-37 payload launches from Space Launch Complex 39A at Kennedy Space Center, Florida, December 17, 2022 (U.S. Space Force/Joshua Conti)



A Framework for Mission Analysis in the Space Planning Process

By Nicholas R. Shaw

The U.S. Space Force (USSF) has a joint integration problem. It provides capabilities that give the military and its partners decisive

advantages in combat. In this way, many USSF missions are inherently “joint.” However, the Space Force is unprepared to contribute to planning

for true joint operations—operations with a significant space nexus where the main effort could easily transition between space and other domains. In such an environment, adversary space systems will be high-value targets that drive action, and friendly space systems will be critical assets that require

Lieutenant Colonel Nicholas R. Shaw, USSF, is Commander of U.S. Space Force’s 4th Electromagnetic Warfare Squadron, Space Delta 3, at Peterson Space Force Base.

protection. Although the Space Force has made significant progress toward establishing Service components at the combatant commands, putting Guardians in a position to support joint force commanders (JFCs), the Service has not yet armed those Guardians with a process to bring space system considerations into joint planning.

Space component commands will have to feed the joint planning process (JPP) and may need to plan and execute independent or joint operations on behalf of a JFC.¹ The Service owes its members doctrine that guides space professionals on how to communicate space planning factors related to the operational environment (OE). Without such doctrine, Guardians will struggle to translate their technical and mission expertise into a format that is easily understood by members of other Services.

The Doctrine Picture

In his *Chief of Space Operations' Planning Guidance*, General John W. Raymond, the Service's first commander, directed the Space Force to use joint planning methodology, in part to prepare Guardians for integration with joint forces.² And when the Service published Space Doctrine Publication (SDP) 5-0, *Planning*, in December 2021, that document reinforced the intent to mesh with the joint force by using the JPP, plus an additional step pulled from Air Force doctrine, as a guide for Guardians to follow.³

Unfortunately, the JPP baseline, now captured in SDP 5-0 as the "Space Planning Process" (SPP), will not meet the future needs of the space domain. Pre-established mission analysis processes and products are geared toward terrestrial operations within well-defined physical boundaries. Even when specifically addressing the space domain, joint planning documents generally fail to look beyond the space segment (the portion of space systems in space), ignoring the terrestrial (Earth-based) and link (electromagnetic spectrum) elements that enable space operations. SDP 5-0 acknowledges the problem, stating, "Spacepower planners should be wary of only considering

space-based solutions to problems," and cites terrestrial and link factors as areas of consideration.⁴ However, the Service doctrine does not give its planners any tools for analyzing and incorporating those factors. Most seriously, neither the joint nor the Service doctrine gives space professionals the responsibility for analyzing the full space systems that are relevant to their OE, regardless of whether segments of those systems are in a JFC's battlespace.

Previous models have been sufficient for an environment with little risk of contested space operations. Moving forward, though, the SPP must contain a unique mission analysis framework to capture the information relevant to space systems and portray it in a usable way to the joint command. Without adjustments to the SDP 5-0 doctrine, Guardians are limited in their approach to mission analysis and will be handicapped in their operations.

The Space Force has the challenge of updating its planning methodology to allow Guardians to fully portray the space common operating picture and analyze space domain threats and opportunities. But the Service must do so while still easily integrating its methodology into joint planning, effects, and intelligence processes.

Moving Beyond the Operational Area

A doctrine that fully accounts for space must break with past norms by addressing the fact that space transcends commanders' boundaries. Planners and analysts must look at space from a systems perspective, ignoring the traditional focus on operational areas. If a threat to operations can be eliminated by targeting a ground station on another continent, that fact is relevant to the local command and should be a part of the mission analysis and decisionmaking process. It is not only U.S. Space Command's role to consider the full space system. Guardians will leverage assets from U.S. Space Command, U.S. Cyber Command, and other resources to examine the total extent of the space domain: terrestrial, link, and orbital segments of all friendly and adversary

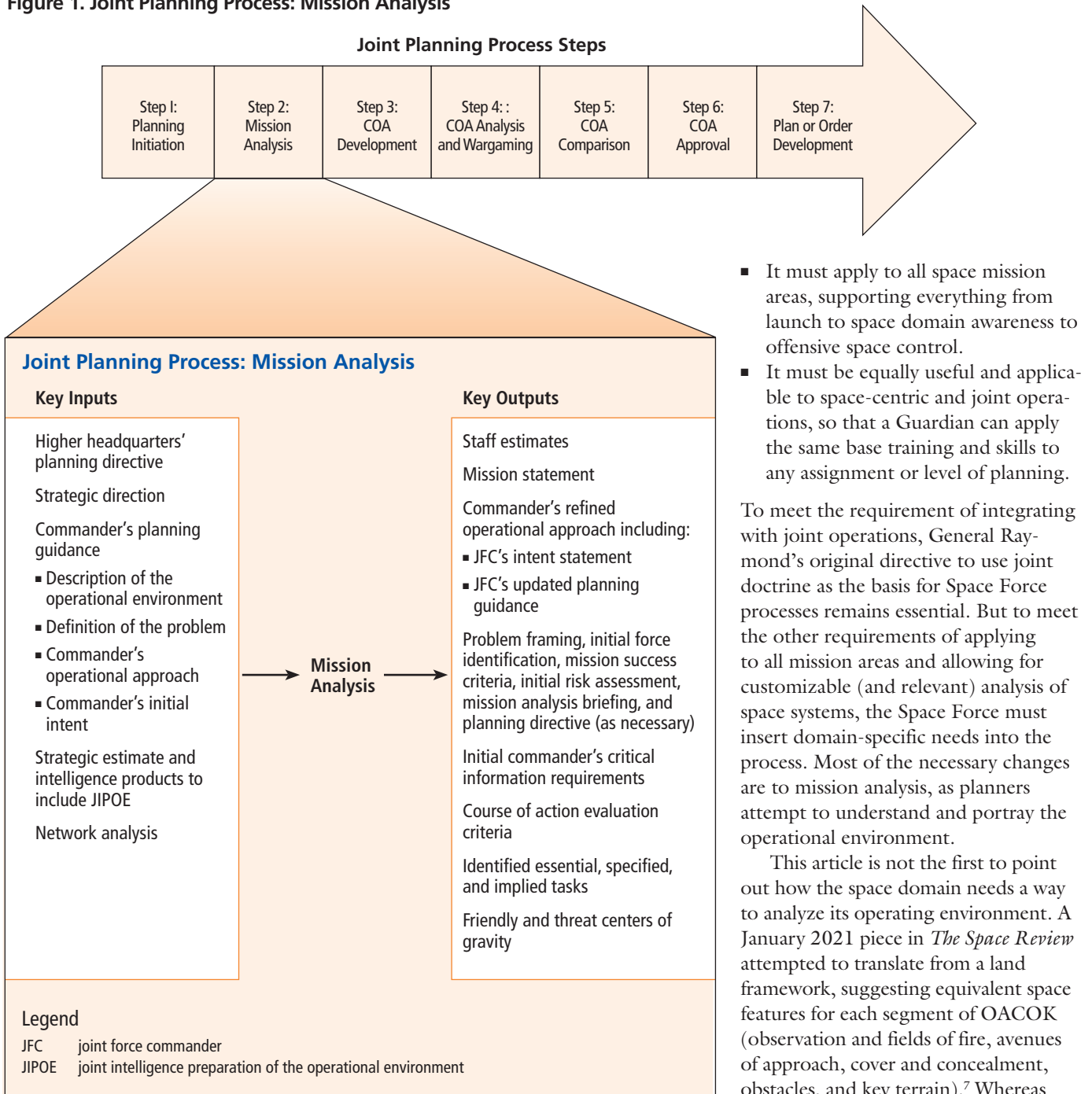
systems that bring effects to their battlespace, wherever elements of the architecture happen to be.

This approach is not an extreme position. For the air domain, an Army analyst may note the presence of an airfield, its length, and general capabilities, but an Air Force operator or analyst will understand the importance of that airfield relative to other sites and the enemy's overall air strategy. An Air Force expert is also the right person to prioritize targeting related to the airfield, rather than the Army expert who "owns" the domain. Similarly, in the maritime domain, a shipyard may be noted on the land component's modified combined obstacle overlay (MCOO), but the Navy should lead on providing an understanding of how that infrastructure fits into friendly or adversary capabilities and the need for action related to it.

For space systems, the ground and link segments—such as a satellite control station and its associated communications frequency to control a space-based asset—may be more accessible or more vulnerable than the space systems they support. Also, it may be acceptable for the Space Force to prioritize targeting the ground and link segments over the space segment, to avoid space debris and to establish precedent for responsible space operations. To do so, the space component commands need full authority to analyze and prioritize the terrestrial and electromagnetic portions of space systems that affect their JFCs.

But even if the right authorities were granted today, the Space Force would remain ill-equipped to deliver the analysis that commanders need. Existing methods of examining, defining, and analyzing the space OE are poorly developed. For example, the joint intelligence preparation of the operational environment (JIPOE) manual contains an example of a space MCOO layer that is woefully inadequate.⁵ This doctrinal layer ignores the worldwide nature of space systems, essentially omits the electromagnetic aspects of space operations, and fails to consider most space operations and their effects on the battlefield. And the Service's own

Figure 1. Joint Planning Process: Mission Analysis



- It must apply to all space mission areas, supporting everything from launch to space domain awareness to offensive space control.
- It must be equally useful and applicable to space-centric and joint operations, so that a Guardian can apply the same base training and skills to any assignment or level of planning.

To meet the requirement of integrating with joint operations, General Raymond's original directive to use joint doctrine as the basis for Space Force processes remains essential. But to meet the other requirements of applying to all mission areas and allowing for customizable (and relevant) analysis of space systems, the Space Force must insert domain-specific needs into the process. Most of the necessary changes are to mission analysis, as planners attempt to understand and portray the operational environment.

This article is not the first to point out how the space domain needs a way to analyze its operating environment. A January 2021 piece in *The Space Review* attempted to translate from a land framework, suggesting equivalent space features for each segment of OACOK (observation and fields of fire, avenues of approach, cover and concealment, obstacles, and key terrain).⁷ Whereas some elements of OACOK, such as key terrain, do translate, others do not. A prime example of the latter is observation and fields of fire, which the author assesses are "almost limitless" in space operations. This analysis is limited and unhelpful but is the natural result of the OACOK framework, which does not guide planners through the detailed on-orbit factors and considerations of space system capabilities that would lead

planning doctrine, firmly rooted in joint techniques, lists several space-centric factors (such as orbital hazards and terrestrial sites) but provides no guidance on how to assess those factors.⁶

Guardians at the new component commands will struggle to integrate with the other services and the JFC's staff as they try to follow the SPP. The Space Force must update the SPP to

enable its personnel to analyze the space domain, feeding operations and the joint force's mission analysis.

A Space Planning Process

A new SPP has three main requirements:

- It must be tailorable, allowing planners to customize their analysis to meet the current mission need.



U.S. Space Force 1st Lieutenant Laura Drapinski, 2nd Space Warning Squadron, front, and Specialist 4 Ariana Gonzalez, 11th Space Warning Squadron, use Space-Based Infrared System Simulator to monitor missile indications during simulated combat operations in U.S. European Command during Space Flag 23-1, at Schriever Space Force Base, Colorado, December 13, 2022 (U.S. Space Force/Judi Tomich)

to true OE analysis. Also, the OACOK model—like other existing models—assumes proximity of elements on the battlefield. It does not account for the distributed systems, remote effects, and reliance on links that define the space domain. Overall, the output from this framework is unusable and is an example of why space analysis must differ from the traditional approach to land, maritime, or air domains.

The Space Force’s model to analyze the OE, providing mission analysis and options to JFCs, must consider all three segments: space, link, and ground. It must look beyond the borders of the physical space domain and beyond the traditional borders of the commands that space forces support. Ultimately, it must provide

in-depth assessments of friendly and adversary space systems—on the ground, at sea, in the air, in space, in cyberspace, or within the electromagnetic spectrum.

A traditional approach to OE assessment starts by addressing the environment separately from the forces employed in it. For example, an Army intelligence analyst would begin by analyzing the battlespace terrain. That Soldier would then set the terrain analysis aside and assess the adversary’s capabilities, purely because of knowledge of the order of battle, assessed objectives, and doctrine. Finally, the analyst would “overlay” the enemy’s likely actions on the terrain, developing courses of action that utilize the terrain features where the operation will take place.

Mission analysis of the space OE cannot follow this pattern, where the environment is examined before considering the forces. Space is *supraglobal* (a term coined by Lieutenant General John E. Shaw, deputy commander, U.S. Space Command, to capture the immense physical area and scope of impact of space operations), and there is no way to start with the local terrain or climate.⁸ Instead, the actual or ideal locations of segments of space systems determine which terrain or weather elements are factors to a space professional. Therefore, analysis of the space OE is a combined process in which the environment and space systems are considered concurrently.

In the JPP, the mission analysis step has a few inputs and outputs, building



Loadmasters from 60th Air Mobility Wing and Lockheed Martin Space unload sixth Geosynchronous Earth Orbit Space Based Infrared System satellite from C-5M Super Galaxy, at Cape Canaveral Space Force Station, Florida, June 2, 2022 (U.S. Space Force/Walter Talens)

the knowledge necessary for development of courses of action and informed decisionmaking by the commander. The figure, derived from Figure III-5 in Joint Publication 5-0, *Joint Planning*, outlines those inputs and outputs.

To integrate with the JPP, the SPP needs to provide the same range of planning outputs from mission analysis. This article proposes the following five-part mission analysis approach in the SPP:

1. frame the mission
2. analyze space systems

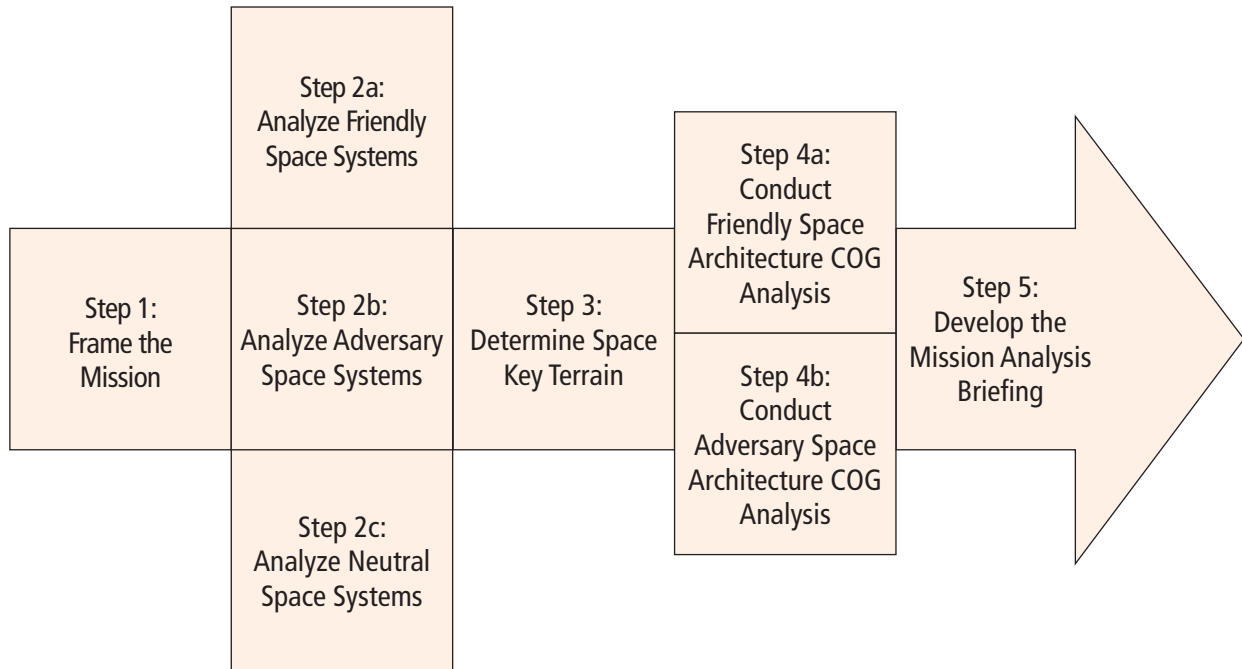
3. determine space key terrain
4. conduct space architecture center-of-gravity (COG) analyses
5. develop the mission analysis briefing.

Step 1: Frame the Mission. Upon receipt of instructions from a higher headquarters or guidance from the commander, the planning staff conducts initial framing of the mission. Guardians identify the specified, implied, and essential tasks and validate that they have a clear understanding of the commander's intent for the operation. They also begin to develop

staff estimates, capturing assets available, constraints, restraints, limitations, facts, assumptions, and other key details from the initial guidance. With these facts, leaders can make informed decisions on which elements of the space domain to analyze and leverage in their planning.

Step 2: Analyze Space Systems. Analysis of space systems determines the scope of the space operational area—the range of effects and architectures relevant to a commander. The ideal way to visualize space systems is through a global, scalable space MCOO with layers of elements.

Figure 2. Space Planning Process Mission Analysis Steps



Layers for consideration in a space MCOO are identified in the table. Development of these layers will feed the assessment of the environment and friendly, adversary, and neutral capabilities in this step and will provide the information needed to complete steps 3 through 5. The specific layers incorporated, analyzed, and provided to the commander's common operating picture are dependent on the operation, allowing it to be tailored to the space mission area or commander's objectives.

Note that for mission planning, specific mission orbits (space segment); the locations of ground stations, spacelift facilities, space observation sites, directed energy systems, or jammers (ground segment); or specific electromagnetic frequencies (link segment) may be notional/ideal to help with the later identification of key terrain for a specific mission. This structure for analyzing the segments of space systems gives space planners a framework for their mission analysis. It is a baseline of training that all members of the Service should receive to contribute to USSF and joint operations. Leaders guide their teams in the execution of planning for specific missions by using the information

provided to them in step 1 of the JPP (planning initiation), together with information from step 1 of the mission analysis process proposed in this article (frame the mission), to identify which layers are needed to shape decisions for the operation at hand. For example, planning for a spacelift mission might require all the layers in the space and link segments but need to look only at the weather and ground station layers of the ground segment. This scalability makes the format tailorable to any situation.

Step 2a: Analyze friendly space systems. Analysis of friendly space systems provides a commander with awareness of current capabilities and limitations. It provides the information necessary for an assessment of the force's own space COG and associated critical capabilities, requirements, and vulnerabilities. Planners conduct analysis of friendly space systems by working through the space MCOO layers, analyzing the environment and friendly capabilities relevant to the operation. Space operations personnel lead the analysis of friendly space systems via cross-functional teams with expertise in all relevant space mission areas.

Step 2b: Analyze adversary space systems. Analysis of adversary space systems

provides a commander with awareness of the enemy's capabilities and limitations. It enables an assessment of the adversary's space COG factors. Commercial or other national systems (spacelift; satellite communications; intelligence, surveillance, and reconnaissance; navigation and timing; other capabilities) known to be used by the adversary should be considered in this step as well. A planner will accomplish analysis of the adversary systems by going through the relevant space MCOO layers with a focus on the adversary's capabilities. Intelligence personnel should lead the examination of the adversary systems. Operations personnel with expertise in each space mission area support the effort.

Step 2c: Analyze neutral space systems. Many commercial entities, nonbelligerent countries, and international partnerships conduct space activities for business, scientific, tourism, or other purposes. As an example of relevant neutral space systems: commercial remote-sensing or satellite communications platforms represent additional capabilities that could be leveraged by friendly or adversary forces. Other satellites may also use critical segments of the electromagnetic spectrum in the commander's battlespace. Analysis of the space OE is incomplete without



Two members of 216th Space Control Squadron set up antennas as part of “Honey Badger System” during Black Skies 22, designed to rehearse command and control of multiple joint electronic warfare fires, at Vandenberg Space Force Base, California, September 20, 2022 (U.S. Space Force/Luke Kitterman)

consideration of these systems. As in assessment of friendly and adversary systems, space planners use the space MCOO layers to complete this step, focusing on neutral space systems that affect the OE. This assessment is led by space operations personnel with expertise from each space mission area.

Step 3: Determine Space Key Terrain. Key terrain is a subset of terrain that provides a distinct military advantage to the side that controls it. Key terrain is dependent on the operation being conducted. Identification of key terrain shapes the development of courses of action (COAs) in future steps

of the JPP and SPP and influences the commander’s decision on which COA will best support the endstate.

Space key terrain is determined by a set of terrain characteristics (based on relative locations and access via space system links) that, at a specific time, provide a distinct military advantage in an operation to the force in control of that terrain. Space planners determine which sets of characteristics should be considered space key terrain through analysis of the operation and their assessments of friendly, enemy, and neutral space architectures.

Key terrain must be controlled to provide an advantage. In space

operations, that control requires placement of a space system object in the right location, at the right time, with an unobstructed path to the target location for desired effects, and the ability to use the portions of the electromagnetic spectrum relevant to the specific mission. If any of these factors is denied, the key terrain is no longer controlled, and there are no advantages to the combatant.

With the identification of specific space key terrain, planners help the commander visualize the critical factors that will influence the outcome of space operations. Identification of the key terrain will also support future requests

Table. Space MCOO Layers

Space Segment (“WeGOTO”)	
We: Space Weather	Space weather/climate impacts on on-orbit systems (does not include uplink/downlink/crosslink or terrestrial comms)
G: Gravity	Gravity “slope” plot, showing changes in potential energy and interactions between celestial bodies
O: Orbit Profiles	Mission orbit(s), characterization, and operational status, as operationally relevant—could include ground tracks and field of view for information, surveillance, reconnaissance satellites; the health of a constellation; or effects of satellite geometry from global navigation satellite system distribution
T: Space Terrain	Space terrain features, such as debris, micrometeorites, and the Van Allen radiation belts. Terrain is captured in mission analysis when the terrain will come within a certain proximity of or overlap with mission orbits
O: Orbit Threats	Co-orbital threats, such as rendezvous proximity operations—capable platforms or other potential adversary capabilities within a certain proximity of mission orbits
Ground Segment (“WeGrASSpED”)	
We: Terrestrial Weather	Terrestrial weather/climate impacts on ground segments
Gr: Ground Stations	Locations of ground stations that enable command and control, uplink/downlink, or other space mission capabilities
A: Anti-Satellite Weapons	Location and characterization of anti-satellite weapons systems
S: Space Observation Sites	Radar or optical sensor sites used by space surveillance networks, and their assessed capabilities (threat fan and detection threshold)
Sp: Spacelift	Locations of spacelift facilities (space access and sustainment sites) that enable delivery of space systems to orbit, and projected spacelift operations (timeline, payload, and destination) from each site
E: Electronic Warfare	Locations of electronic warfare systems, such as jammers or spoofing systems, and their assessed capabilities (frequencies, power, and likely area of effects)
D: Directed Energy Weapons	Directed energy sites for space control, and their assessed capabilities (threat fan and potential impacts)
Link Segment (“WeFI”)	
We: Weather	Space or terrestrial weather/climate impacts on uplink/downlink/crosslink signals (location, duration, and anticipated effects)
F: Frequencies	Link electromagnetic factors for space systems (frequency and vector, for both control and payload mission)
I: Interference	Any known friendly, enemy, or neutral systems operating on the same frequencies that could result in intentional or unintentional jamming

for collection, targeting, or protection related to these terrain features.

Step 4: Conduct Space Architecture COG Analyses. Using the data now available from analysis of the space systems and assessment of key terrain, planners utilize traditional methods to determine the COG and associated critical capabilities, requirements, and vulnerabilities of the friendly and adversary space architectures. No new system is needed for this mission analysis step; Guardians can utilize joint processes to support interoperability with the rest of the force.

Step 4a: Conduct friendly space architecture center of gravity analysis. Space operations planners perform a self-assessment of the friendly space

architecture. The COG, critical capabilities, critical requirements, and critical vulnerabilities identified during this step help the commander to shape the friendly force information requirements and essential elements of friendly information and to consider investments in protection or redundancy in critical elements of the space systems.

Step 4b: Conduct adversary space architecture COG analysis. The adversary’s space architecture receives the same attention, with planners identifying the adversary’s space COG, critical capabilities, requirements, and vulnerabilities for exploitation. Assessment of the adversary’s COG is led by the intelligence staff. These items will shape the development

of COAs, support prioritization of targets, and contribute to the development of priority intelligence requirements.

Step 5: Develop the Mission Analysis Briefing. The previous SPP mission analysis steps generate the extensive data needed to update and refine the initial JIPOE product and complete drafts of staff estimates. The products are translated into the mission analysis briefing, continuing the dialogue between the staff and the commander. In this step, the other JPP mission outputs that were not covered in previous SPP mission analysis steps, such as development of a proposed mission statement, initial risk assessment, and COA consideration criteria, are completed and incorporated into the briefing.

SpaceX Falcon 9 reusable, two-stage rocket from Vandenberg Space Force Base, California, launches first set of Space Development Agency's Tranche 0 of Proliferated Warfighter Space Architecture satellites, April 2, 2023 (SpaceX)



Up until this point in the SPP mission analysis framework, the planning staff has collaborated in the development of a single MCOO, a combined list of proposed space key terrain, and mutually assessed COGs. Now, all members of the space planning staff have the information they need to tailor their sections' own products. The core mission analysis products serve as a launching point for the development of sustainment plans, the drafting of COAs, the maintenance of running estimates, and other actions by the staff.

With the employment of this adjustment to the SPP, the elements unique to space planning have been addressed and planners can merge with the traditional process, continuing with JPP step 3 (COA development). Following this series of steps and guidance satisfies the three requirements (tailorable, applicable to all space missions, and universally applicable to space-centric or joint operations) identified at the beginning of this section and enables space planners to meet their domain-specific needs.

Overall, the products that result from this five-step SPP mission analysis process will provide a picture that spreads far beyond a single operational area, potentially hitting multiple combatant commands and orbital regimes. But through its execution, space planners and analysts will obtain the data they need to present a complete picture to the commander for assessment of friendly and adversary capabilities and COGs, decisions on targeting or protection of space system segments, selection of a COA, and initiation of necessary coordination with supporting or supported commands.

Calls to Action

The process as outlined above would meet the needs of the growing Service, but there are three major prerequisites for the Space Force to successfully adopt this model as an update to its SDP 5-0 doctrine. Those prerequisites involve process validation, data management, and training integration. No new process can be adopted with confidence unless it has been questioned and tested by experts from across the space mission

areas. Space planners should critically validate this SPP recommendation, testing it against their mission areas to identify gaps and confirm its utility. Where possible, they should provide feedback to simplify the framework, making it easier for Guardians to learn and implement.

The framework outlined in this article involves the processing and display of a huge amount of data. The three-dimensional nature of space systems makes it even more difficult to accomplish. Visualization tools to display the space MCOO are not available yet; space planners will have to utilize local innovation and alternative products to portray their analysis until the optimal resources are fielded. The Space Force's vision of a digital service is needed here, and quickly, to turn these immense requirements into a user-friendly interface that allows for rapid, customizable presentation of the relevant data. The systems that display this information must communicate with the mission command systems used in the joint community, allowing Guardians to seamlessly shift their products into a joint display of the OE for mission planning purposes. Without that essential step by the Service's innovation teams, it will be virtually impossible for a space planner to convey analysis to a decisionmaker.

Finally, capturing this planning model in Service doctrine (SDP 5-0, SDP 2-0, and associated implementation documents) is only one part of the transition. The Space Force must train Guardians in its use for application at the combatant commands and in core space mission assignments. Only by integrating this methodology into the Service's beginning education, reinforcing the process in later schools, and leveraging the SPP for space planning in all organizations can the Space Force build a cadre of planners capable of supporting joint operations.

The USSF's transition from a traditional role, with space operations focused on "space for others," to a component role in joint operations requires an investment in personnel and processes. The mission analysis framework proposed

here will support the establishment of the Space Force as an equal member of the joint planning team. Testing of this process, followed by its inclusion in Service doctrine and education and the development of supporting visualization aids, is necessary for the Space Force's growth and ownership of the domain. The Space Force is approaching an exciting milestone with its establishment of component commands. It is imperative that Guardians across the force have the knowledge and tools to succeed in their new roles. JFQ

Notes

¹ Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017), VIII-21.

² John W. Raymond, *Chief of Space Operations' Planning Guidance* (November 9, 2020), 9, available at <<https://media.defense.gov/2020/nov/09/2002531998/-1/-1/0/cso%20planning%20guidance.pdf>>.

³ Space Doctrine Publication (SDP) 5-0, *Planning* (Peterson Space Force Base, CO: Space Training and Readiness Command, December 2021), 12.

⁴ *Ibid.*, 9.

⁵ JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment* (Washington, DC: The Joint Staff, May 21, 2014), III-20, available at <<https://irp.fas.org/doddir/dod/jp2-01-3.pdf>>.

⁶ SDP 5-0, *Planning*, 16–18.

⁷ D. Grant Greffey, "Terrain Analysis for Space Warfare," *The Space Review*, January 25, 2021, available at <<https://www.thespacereview.com/article/4111/1>>.

⁸ John E. Shaw, Jean Purgason, and Amy Soileau, "Sailing the New Wine-Dark Sea: Space as a Military Area of Responsibility," *AEther* 1, no. 1 (Spring 2022), available at <https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-1/06-Shaw.pdf>.

CALL FOR ENTRIES

for the

2023 Secretary of Defense and
2023 Chairman of the Joint Chiefs of Staff

Essay Competitions

Are you a professional military education (PME) student? Imagine your winning essay published in a future issue of *Joint Force Quarterly*, catching the eye of the Secretary and Chairman as well as contributing to the debate on an important national security issue.

Who's Eligible? Students, including international students, at U.S. PME colleges, schools, and other programs, and Service research fellows.

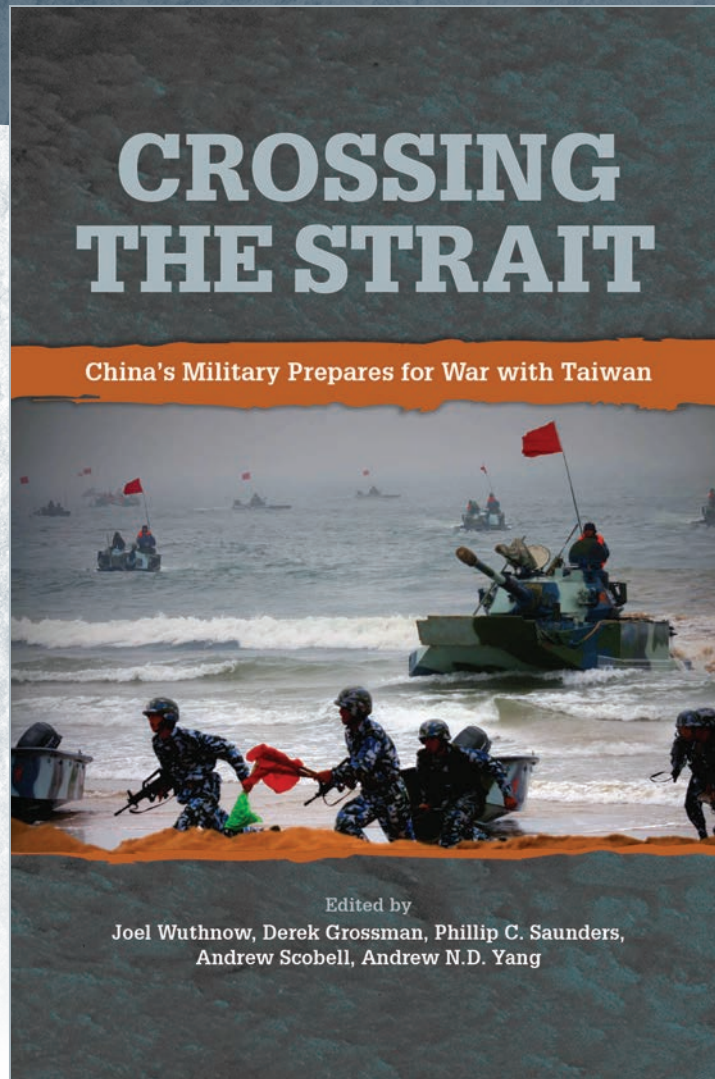
What's Required? Research and write an original, unclassified essay on some aspect of U.S. national, defense, or military strategy. The essay may be written in conjunction with a course writing requirement. Important: Please note that entries must be selected by and submitted through your college.

When? Anytime during the 2022–2023 academic year. Students are encouraged to begin early and avoid the spring rush. Final judging and selection of winners take place May 11–12, 2023, at NDU Press, Fort McNair, Washington, DC.

For further information, see your college's essay coordinator or go to:
<https://ndupress.ndu.edu/About/Essay-Competitions/>

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

HOME COVID-19 GUIDANCE ABOUT JOURNALS PUBLICATIONS SUBMIT A MANUSCRIPT CONTACT

Search NDU Press

The Quantum Internet: How DOD Can Prepare

The future viability of a quantum Internet could shape the strategic environment for U.S. military forces.

[Read More →](#)

The premier professional military and academic publishing house of the National Defense University

STRATEGIC PERSPECTIVES 29 | MARCH 25, 2019
Russian Challenges from Now into the Next Generation: A Geostrategic Primer
Peter B. Zwack and Marie-Charlotte Pierre

JOINT FORCE QUARTERLY 104 | DEC. 29, 2021
Health, Pandemic Preparedness, and Multidomain Operations
Samir S. Deshpande, Amy B. Adler, Susan P. Proctor, Vincent F. Capaldi, James P. McClung, Toby D. Elliman, and Deydre S. Teyhen

PRISM VOL. 9, NO. 3 | NOV. 18, 2021
The Pentagon's First Financial War
Justin Bernier

JOINT FORCE QUARTERLY 104 | DEC. 29, 2021
Defending Taiwan in an Expanded Competitive Space
Joel Wuthnow

You can also find us on:



Twitter



Facebook



JOINT FORCE QUARTERLY
Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

