



**JFQ**

**Joint Force Quarterly**

Issue 105, 2<sup>nd</sup> Quarter 2022

## **The Quantum Internet**

An Interview with Richard D. Clarke

Toward Military Design

# Joint Force Quarterly

Founded in 1993 • Vol. 105, 2<sup>nd</sup> Quarter 2022  
<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

**Copyeditor**

Andrea L. Connell

**Book Review Editor**

Brett Swaney

**Creative Director**

John Mitrione, *U.S. Government Publishing Office*

**Contract Copyeditor**

Shira Klapper

**Advisory Committee**

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; Col Lee G. Gentile, Jr., USAF/Air Command and Staff 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 Michael D. Lundy, USA/U.S. Army Command and General Staff College; MG Stephen J. Maranian, USA/U.S. Army War College; BG Voris McBurnette, USAR/Joint Forces Staff College; VADM Stuart B. Munsch, USN/The Joint Staff; LTG Andrew P. Poppas, USA/The Joint Staff; Brig Gen Michael T. Rawls, USAF/Air War College; Col Blair Sokol, USMC/Marine Corps War College; Col Bradford W. Tippet, USMC/Marine Corps Command and Staff College

**Editorial Board**

Richard K. Betts/Columbia University; Eliot A. Cohen/The Johns Hopkins University; Richard L. DiNardo/Marine Corps Command and Staff College; Aaron L. Friedberg/Princeton University; Bryon Greenwald/National Defense University; COL James E. Hayes, USA/National War College; Douglas N. Hime/Naval War College; Paul J. Springer/Air Command and Staff College; Bert B. Tussing/U.S. Army War College

Cover 2 images (top to bottom): Air Force Staff Sergeant Lael Darrett, 332<sup>nd</sup> Expeditionary Maintenance Squadron crew chief, stands on ladder of F-15E Strike Eagle, October 16, 2021, at undisclosed location in Southwest Asia (U.S. Air Force/Cameron Otte); Army paratrooper assigned to Utah National Guard prepares for joint jump with Utah National Guard's 19<sup>th</sup> Special Forces Group (Airborne) and Royal Moroccan army paratroopers at Ben Guerir Air Base, Morocco, June 10, 2021, as part of African Lion 2021 (U.S. Army/Rhianna Ballenger); Navy Airman Kateryna Trach mans rails aboard aircraft carrier USS *Theodore Roosevelt* as ship returns to Naval Air Station North Island, San Diego, May 25, 2021 (U.S. Navy/Pyoung K. Yi)



# In This Issue

## Dialogue

- 2 Letter to the Editor

## Forum

- 4 Executive Summary
- 6 The Quantum Internet:  
How DOD Can Prepare  
*By Lubjana Beshaj, Samuel Crislip, and Travis Russell*
- 14 Fog of Warfare: Broadening U.S.  
Military Use-of-Force Training  
for Security Cooperation  
*By Patrick Paterson*
- 23 BeiDou: China's GPS  
Challenger Takes Its Place  
on the World Stage  
*By David H. Millner, Stephen Maksim, and Marissa Huhmann*

## Special Feature

- 32 An Interview with  
Richard D. Clarke
- 37 Rediscovering the Value  
of Special Operations  
*By Isaiah Wilson III*
- 44 Making the Case for a Joint  
Special Operations Profession  
*By Isaiah Wilson III and  
C. Anthony Pfaff*
- 55 What Is JSOU? Then,  
Now, and Next  
*By David M. Dudas, Bethany Fidermutz, and Amie Lonas*

## Features

- 60 Persistent Knowledge Gaps in  
the Chinese Defense Budget  
*By Frederico Bartels*
- 69 U.S. European Command  
Theater Infrastructure Plan:  
Aligning U.S. Requirements  
with European Capability  
and Resources  
*By Jon-Paul Depreo and  
Scott P. Raymond*
- 75 All Quiet on the Eastern Front:  
NATO Civil-Military Deterrence  
of Russian Hybrid Warfare  
*By Andrew Underwood, Andrew Emery, Paul Haynsworth,  
and Jennifer Barnes*



## About the Cover

Staff Sergeant Justin McNeil from 3<sup>rd</sup> Battalion, 161<sup>st</sup> Infantry Regiment, repacks his parachute after dropping into Houtdorperveld Drop Zone, in Netherlands, during exercise Falcon Leap, September 16, 2021 (U.S. Army National Guard/Remi Milslagle)

## Recall

- 86 Improvised Partnerships:  
U.S. Joint Operations in the  
Mexican-American War  
*By Nathan A. Jennings*

## Book Reviews

- 95 Leap of Faith  
*Reviewed by Andrew J. Forney*
- 96 The Black Banners (Declassified)  
*Reviewed by Bryon Greenwald*
- 97 Shields of the Republic  
*Reviewed by James J. Townsend, Jr.*

## Joint Doctrine

- 99 Toward Military Design: Six  
Ways the JP 5-O's Operational  
Design Falls Short  
*By Andrew L. Crabb*
- 104 Joint Doctrine Update

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

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

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

### Copyright Notice

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

### Submissions and Communications

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

### Editor, *Joint Force Quarterly*

NDU Press  
300 Fifth Avenue (Building 62, Suite 212)  
Fort Lesley J. McNair  
Washington, DC 20319  
Telephone: (202) 685-4220/DSN 325  
Email: [JFQ1@ndu.edu](mailto:JFQ1@ndu.edu)  
*JFQ* online: [ndupress.ndu.edu/jfq](http://ndupress.ndu.edu/jfq)  
2<sup>nd</sup> Quarter, April 2022  
ISSN 1070-0692

# Letter to the Editor

In 1995, while one of a handful of Black students at the National War College (NWC) at Fort Lesley J. McNair in Washington, DC, I requested to attend the Million Man March, which was being held in Washington on Friday, October 16, 1995. As a young man from Louisville, Kentucky, who came to the Marine Corps via Annapolis, I had wanted to attend this historical event and to join my brother, Rodney K. Dunn, who was traveling in from Columbus, Ohio. The Million Man March has proved to be a historical, iconic event for our entire country.

NWC had a scheduled field trip to the Gettysburg Battlefield for that day. I had visited there four times prior to this trip and had taught the battle sequence while an instructor at the Marine Corps' Amphibious Warfare School (now the Expeditionary Warfare School) from 1984 to 1986. My request was turned down. I recall traveling on the bus going north that Friday morning and the cascade of buses coming south, heading to the National Mall. The contrasts of that Friday morning have stayed with me over the years.

Clearly, professional military education (PME) core instruction and teaching do not appear to have kept pace with racial diversity within the Services. In 1995, it was not even a consideration to allow me to attend that march. A reason may have been because the NWC faculty was not a diverse faculty and had no appreciation for the Million Man March, so my request did not stand a chance.

Fast-forward to 2020. Most PME institutions are taught by majority white faculty members still, with some staffed completely by white men and women. Without a diverse faculty, course content will reflect the same lack of diversity. But now the Services have the window of opportunity to change this woeful situation.

The impact of PME cannot be overstated. All future generals, admirals, and many Senior Executive Service members attend these prestigious institutions. I attended NWC, then after graduation taught across the campus at the Industrial College of the Armed Forces (ICAF), now the Eisenhower School. In effect, I had the best of both: national security strategy at NWC and national resources strategy at ICAF. Both were serious academic powerhouses, with one distinct difference outside of their mission statements: NWC was taught by an all-white, mostly male faculty, while ICAF was taught by a racially diverse faculty with women filling significant faculty positions. ICAF had a solid emphasis on ensuring that the rich history of our military's diversity was taught to all students. I was a member of that prestigious faculty for 2 years.

This past year, one of the more significant initiatives that former Secretary of the Navy, Thomas Modly, had introduced was his "Vector" series of changes. Vector 13 was a wholesale change in PME taught by the Navy and Marine Corps. Secretary Modly called for the implementation of a Naval Community College and other initiatives that would require hiring more faculty, teaching, and administrative positions. I saw this as an opportunity to finally change PME by hiring diverse faculty members and enhancing curricula throughout these schoolhouses to reflect the rich cultural history of our Services and organizations. His resignation may have stalled this initiative. I hope not.

Ensuring all our military students are taught subjects that include an acknowledgment of the rich diversity that exists in our military and the cultures of foreign militaries means that we are operating in a more realistic world.

It is time for a thorough review of our PME taught by all the Services with the thought of improving the academic and practical approaches to winning the next battle. I recommend that NWC and all war colleges be required to take a time out to consider what is happening *now* and be compelled to write a way ahead that will improve race relations in our Services and society. Unless they do, the foundation of our national security will erode precipitously.

I was a student 25 years ago. PME has not kept abreast with the national security imperative to eliminate the toxicity of institutional bias and discrimination. JFQ

Kenneth D. Dunn, Ed.D.  
Colonel, USMC (Ret.)  
U.S. Naval Academy, 1974  
NWC, 1996  
Military Professor, ICAF, 1996–1998



The Million Man March, October 16, 1995, in Washington, DC (Mark Reinstein)



Medal of Honor recipient  
Army Captain Humbert  
Roque "Rocky" Versace  
(U.S. Army)

## Executive Summary

**O**n a rainy spring day here on the Potomac, the war in Ukraine rages on, and what can be done is being done. Ukrainians are showing the world what real courage is as Russia wages a brutal war against them. While Thomas Hobbes told us that life is “solitary, poor, nasty, brutish, and short,” war is certainly all those things and more. The pain of war spreads out widely in the obvious ruins of lives lost, cities leveled, homes and businesses destroyed, and futures

denied. Russia’s invasion of Ukraine, on February 24, 2022, will be remembered by millions of people, like some of us remember 9/11 or December 7, or the fateful early July days of 1863, at Gettysburg, Pennsylvania.

After the end of the Civil War, the names of Confederate leaders eventually graced 10 Army installations, which until recently was not really questioned. The rationale was both political and a part of where we were as a society. But today, after nearly 160 years, attitudes are changing.

I see an obvious issue that is soon to be resolved by the Department of Defense (DOD), which will likely be disputed despite the diligent and careful work that has been done to make a positive change: renaming military bases. By law, these bases must have new names by January 1, 2024. While some say vestiges of our Civil War are heritage that should be respected, DOD has already settled that part of the issue, and these bases will be renamed.

If you study our country’s history, you gain perspective, and that viewpoint

is not always validating to your beliefs. Hopefully, you see the need to do better as a citizen. Those once seen as heroes were only men who sought to achieve what they wanted to hold on to, including other humans whom they did not see as equals.

One of the 87 names recommended by the Naming Commission (a congressional commission that “has the important role of recommending names that exemplify . . . U.S. military and national values”) caught my eye: Captain Humbert Roque “Rocky” Versace, the son of an Army officer and West Point graduate, himself a 1959 West Point graduate, who eventually served as a special operations intelligence advisor in the early days of the Vietnam War. As a POW, he took command in a hidden jungle prison of cages exposed to the elements and did all he could to resist, a truly awe-inspiring example of courage as he dealt with unspeakable acts of torture. His body was never recovered but was announced as being executed by his Vietnamese captors.

He was awarded the Silver Star but deserved the Medal of Honor, which was eventually awarded posthumously by President George W. Bush in 2002. His fellow POWs who witnessed his courage, bravery, and faith returned home and established the first Survival, Evasion, Resistance, and Escape (SERE) training organization to help others deal with similar situations in future combat. His friends also erected a permanent memorial to Captain Versace near Old Town Alexandria, Virginia. You should know his story. He was the first Army POW in Vietnam so awarded a Medal of Honor.

If you know Rocky’s story of courage and the stories of the other people on the list, and you know why these bases were named such, can you honestly say an officer who took up arms against the United States deserves such an honor? Especially now, as we see others fighting for the same freedoms that we often take for granted. Our Civil War must end, lest we continue to repeat the mistakes of the past. We do not want to end up like Russia, with an “alternative history” that just leads to more bloodshed.

The Forum brings a wide range of ideas, from the future of the Internet to security cooperation training to dealing with China’s navigation satellites. Looking at the Internet in the years ahead, Lubjana Beshaj, Samuel Crislip, and Travis Russell describe how the quantum Internet is arriving, what that means, and what DOD should do to prepare. As the U.S. military has found itself engaged in many conflicts short of war in a conventional sense, Patrick Paterson discusses how the joint force, which tends to follow the Law of Armed Conflict, can best assist our partners who are likely using procedures in line with criminal and human rights laws. After launching BeiDou, China now has its own GPS-like satellite constellation, and David Millner, Stephen Maksim, and Marissa Huhmann discuss the impact on the global use of such systems.

Often the stuff of blockbuster movie plots that tend to overdramatize the intense and focused missions of special forces, we bring you a Special Feature focusing on today’s U.S. Special Operations Command (USSOCOM). In my interview with General Richard D. Clarke, USA, the 12<sup>th</sup> commander of USSOCOM, we discuss where this unique combatant command is today and where it is headed. A key part of the command’s mission is training and education, which General Clarke has focused on in a reset of the Joint Special Operations University (JSOU). The new president of JSOU, Isaiah (Ike) Wilson III, and coauthor Anthony Pfaff of the U.S. Army War College, offer a perspective on the importance of today’s special operations as a part of our nation’s defense. While the Services contribute forces to USSOCOM to perform its missions, Dr. Wilson and Dr. Pfaff describe how individuals in these special operations forces should consider such work as a *profession* within the profession of arms. Unique within the combatant commands, USSOCOM has an educational institution that is transitioning from primarily being a short-course training mission to becoming a member of the U.S. joint professional military education institutions. David Dudas,

Bethany Fidermutz, and Amie Lonas take us inside JSOU for a closer look.

As each issue of *JFQ* is developed months in advance of publication, events sometimes outpace what our authors write about, as is the case with the Russian war in Ukraine. In Features, we have an important article on the Chinese budget and two pieces from the European theater that still hold up as important reads. There is an old saying—that to understand a nation’s intent, simply look at its budget—and Frederico Bartels helps us see the difficulty in doing so with China’s defense spending. Two experts from U.S. European Command, Jon-Paul Depreo and Scott Raymond, help us see that infrastructure planning within the command is aligned with European Allies and other partners. As we are seeing play out, these efforts are showing value as the North Atlantic Treaty Organization (NATO) defends against Russia. The title of Andrew Underwood, Andrew Emery, Paul Haynsworth, and Jennifer Barnes’s article that discusses how NATO would defend against Russia might seem off a bit, but from a warfighting perspective the Alliance is holding its own.

Recall and Joint Doctrine respectively bookend the past and the future of U.S. joint warfighting. In Recall, Nathan Jennings examines the Mexican-American War and provides a pre-historic view of joint operations, one I would offer that then Captain U.S. Grant, who was in that campaign, would have in mind during the Western Campaign of 1862–1863 culminating in the victory at Vicksburg, a very joint affair. Andrew Crabb next offers his critique of Joint Publication 5-0, *Joint Planning*, in terms of operational design. We close this issue with three valuable book reviews and our Joint Doctrine Update.

In these difficult times, I hope each of us can see new ways to work together to seek a better world, both at home and around the world. *JFQ*

—William T. Eliason,  
Editor in Chief



National Institute of Standards and Technology physicist Katie McCormick adjusts mirror to steer laser beam used to cool trapped beryllium ion, as part of efforts to improve quantum measurements and quantum computing, October 26, 2018 (National Institute of Standards and Technology/James Burrus)

# The Quantum Internet

## How DOD Can Prepare

By Lubjana Beshaj, Samuel Crislip, and Travis Russell

In the 1980s, Richard Feynman famously posed the idea of a computer that harnessed the power of quantum mechanics to carry out calculations.<sup>1</sup> Feynman observed that the computers of his day had a difficult time modeling complex molecular systems. He observed that if the computer harnessed the laws of quantum mechanics, it could easily model such molecular systems.

By the mid-1990s, the concept of a quantum computer was well established in academia, and at that time mathematician Peter Shor discovered a polynomial-time algorithm for factoring large integers on one.<sup>2</sup> It was soon observed that such an algorithm, by quickly computing keys for decryption, would break many widely used encryption schemes previously considered secure.

Recent advances in quantum technology made by state and private actors transformed the quantum computer from an idea to working prototype. Although a computer capable of carrying out Shor's algorithm is likely still years away, stakeholders in government and industry have largely accepted the need to prepare for a quantum future. The most obvious feature of this preparation is the race by the National Institute of Standards and Technology and others to produce secure postquantum cryptographic schemes that are unlikely to be impacted when full-scale quantum computing comes to fruition.<sup>3</sup> Less attention has been paid,

---

Dr. Lubjana Beshaj is a Cyber Fellow of Mathematics in the Army Cyber Institute and an Assistant Professor in the Department of Mathematical Sciences at the United States Military Academy (USMA). Command Sergeant Major Samuel Crislip, USA, is Command Sergeant Major at the 782<sup>nd</sup> Military Intelligence Battalion Command in Fort Gordon, Georgia. Dr. Travis Russell is a Research Scientist in the Army Cyber Institute and an Assistant Professor in the Department of Mathematical Sciences at the USMA.



however, to the infrastructure that will need to be in place to support a network of active quantum computers. Such a network is commonly referred to as the *quantum Internet*.

In this article, we discuss how the quantum Internet is likely to develop, according to experts. Following the model proposed by Stephanie Wehner, David Elkouss, and Ronald Hanson, we break this development into six stages.<sup>4</sup> Each stage introduces a new technology that makes the Internet “more quantum” than it was at the previous stage. As we discuss each development, we draw the reader’s attention to technologies and trends of interest to the Department of Defense (DOD). We argue that increasing DOD focus on quantum technology and a viable quantum Internet may lead to innovations in the areas of secure communications, quantum sensing, and clock synchronization, as well as other yet-to-be-discovered technologies.

We wish to emphasize that this article elaborates on the model proposed by Wehner, Elkouss, and Hanson but does not propose an alternative version, though other models may well exist, and the actual way in which a quantum Internet may develop is entirely unknown. The six stages we describe are such that, at each stage, a new technology is introduced that addresses a vulnerability of the previous stage. In this article we do not address the potential costs or returns on investments in these technologies; we describe the technologies only qualitatively. We also do not speculate when these technologies will be widely available, as there is ample conjecture on this question in the literature.

The future viability of (and accessibility to) a quantum Internet could shape the strategic environment for U.S. military forces. This environment comprises the critical operational areas in which DOD finds itself during competition, conflict, or combat. These operations are known, sometimes interchangeably, as multidomain or all-domain operations (MDO/ADO). Joint doctrine currently recognizes land, sea, air, space, and cyber as the warfighting domains within MDO/ADO.<sup>5</sup> A quantum Internet is

especially applicable to the cyber domain, as it requires many of the current physical components of the Internet—while necessitating an expansion of many of those assets and an inclusion of new technologies. As DOD and the U.S. Government invest in developing a quantum Internet or securing their access to it, they will witness a growth in their cyber domain capabilities, which, due to the interwoven nature of MDO/ADO, will translate to gains in the other warfighting domains.

### Quantum Technology and the Quantum Internet

For our purposes, the term *quantum Internet* refers to any network of computer systems or communication devices that employ technologies that are inherently quantum. It does not necessarily refer to a new Internet separate from the current one; rather, the term refers to an emerging infrastructure that will be intertwined with the existing Internet. A quantum Internet would likely be necessary to carry out communication between fully operational quantum computers once that technology has developed; however, we see that a quantum Internet would enable much more than the integration of quantum computers, which might not be realized for many years. A quantum Internet, or even the addition of quantum components to the existing Internet, allows for the future integration of quantum computers into the existing Internet and makes possible the transfer and storage of an entirely new kind of information, known colloquially as *quantum information*. Whereas classical information is encrypted and stored as sequences of bits—that is, strings of 0s and 1s—quantum information is encoded in the state of a system of quantum bits, or qubits. A single qubit is the quantum state of a particle in a superposition of a pair of possible states, which is often regarded as a mixture of 0 and 1. In practice, qubits are often encoded as the polarization of a photon or the spin of an electron, though other possibilities have been studied. With access to multiple qubits, the entire system could become “entangled” so that the state of one qubit is closely cor-

related with the state of another (potentially remote) qubit. In this way, computations carried out on separate qubits in distant locations may instantaneously interfere and affect one another.<sup>6</sup>

The laws of quantum mechanics endow quantum information with many properties that distinguish it from classical information and make new applications possible. For example, the no-cloning theorem of quantum mechanics makes it impossible to design an apparatus that takes as input a qubit and produces as output two copies of the same qubit. In other words, an eavesdropper who intercepts a qubit in transit cannot copy the qubit and send the original to its destination undetected. Moreover, the measurement principle of quantum mechanics implies that if an eavesdropper measures any property of a qubit in transit, the state of the qubit will change. Such change could be detected on receipt so that manipulated qubits could be discarded. Entanglement makes possible many other applications, such as new clock synchronization protocols and taking advantage of existing correlations between remote entangled qubits.<sup>7</sup> In summary, a quantum Internet has the potential to alter not only the infrastructure of the cyber domain but also the nature of the information stored and transmitted within that infrastructure.

Although the exact process by which the existing Internet will evolve into a quantum Internet is unknown, experts have recently weighed in on what the process might entail.<sup>8</sup> In the following pages, we describe six stages of development that are predicted to occur as the quantum Internet emerges. At each stage a new technology is introduced that enables significantly more functionality to the quantum Internet. In addition to a summary of these stages, we offer commentary concerning how new technologies introduced at each stage could affect the interests of DOD and what steps the department might consider taking to implement these technologies. We also note which technologies already exist and how different private and government actors have invested in them.

## Trusted Repeater Stage

At the first stage of the development of the quantum Internet, the Internet continues to transmit only classical information; however, it could do so more securely by incorporating quantum repeaters into the existing infrastructure. At this stage, a pair of quantum repeaters requires only the ability to perform a single quantum protocol, namely quantum key distribution (QKD; see figure 1). This protocol allows for the generation of a secret key that is securely distributed to adjacent quantum repeaters.<sup>9</sup> A classical message could then be encoded at one repeater, securely transmitted to the next repeater, and finally decoded. This process could be carried out between each pair of consecutive repeaters, each generating a new secret key, ensuring the transmission of the classical message from source to destination by chaining together multiple repeaters. The term *trusted repeater* stems from the requirement that the message be decodable at each repeater. Hence, secure transmissions rely on the trustworthiness of the sequence of repeaters. The advantage of sending information this way is that the security of the message is guaranteed between repeaters, even in the presence of an eavesdropper. The message could not be decoded without the secret key, and the security of the distribution of the secret key between repeaters is guaranteed by the laws of quantum mechanics rather than the computational difficulty of the decryption process. In other words, an intercepted message could

not be decoded except by guessing the key, now or in the future, even with the aid of a powerful computer or even a quantum computer.<sup>10</sup>

Investment in the trusted repeater stage is critical for DOD as it promotes secure communications that overcome traditional adversarial interception techniques. Military application of this stage would enable geographically separated commanders and subordinates to communicate operational details without concern of interception. This state provides an increase in battlefield overmatch capacity and might also promote a defeat in traditional direction-finding, a method of intercepting communication paths to track the originator's location or signal intercept techniques. This stage would also alert those in the communication chain of attempts to access those secure transmissions, thus "sounding an alarm" so appropriate action can be taken to prevent further interception efforts. Ultimately, increasing security, defeating interception, and reducing or eliminating transmitter detection allow a commander and his or her forces a more secure environment and offer a greater chance of success.

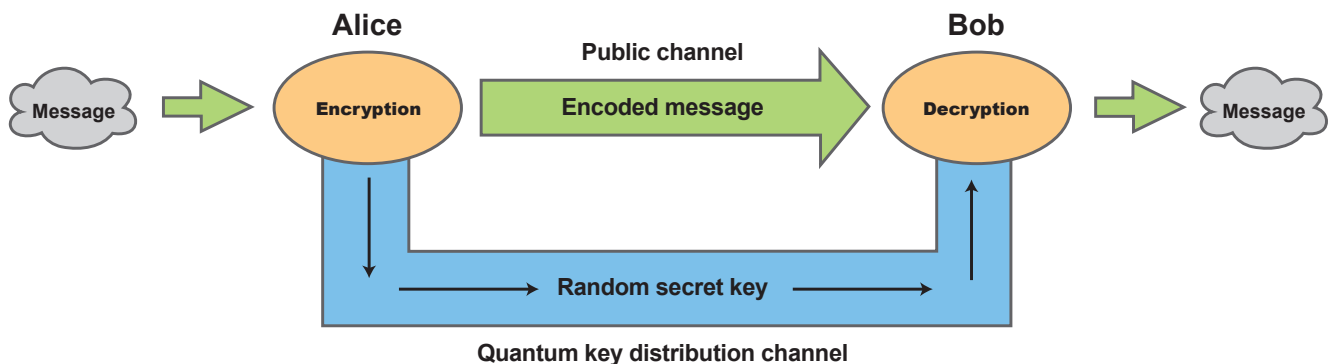
If DOD focuses on increasing capacity for trusted repeaters, it might also promote more secure intelligence transmission in deployed environments rather than rely on traditional intelligence networks. Traditional intelligence transmission techniques depend on complex secure networks that can be arduous in combat operations. Although an option to communicate intelligence through traditional means exists, such methods often require encryption, dedicated

transmission channels, and considerations for the use of coded words or values—all of which delay receipt of intelligence. This impediment could be detrimental to a commander's decision-making cycle, upsetting the efficacy of intelligence while potentially forcing decisions without essential information. A quantum Internet with trusted repeaters, however, could provide the necessary expeditious and secure intelligence transmission environment that commanders would need in a combat environment.

## Prepare-and-Measure Stage

At the second stage of the quantum Internet, the Internet can prepare a single qubit at an initial node and transmit it to a final node where it could be measured. This is the first stage at which the Internet could truly be considered *quantum*, in the sense that it is now able to transmit information in the form of qubits. It is important to note that successful qubit transmission is not likely at this stage. Because of the potential for a qubit to be lost, the receiver must detect whether the qubit has been received before measuring it; hence, all measurements are "postselected" on the knowledge that the qubit was successfully transmitted. The requirement to detect successful transmission implies some limitations on the set of protocols that could be performed, as any measurement of the qubit necessarily perturbs its state.<sup>11</sup> Nonetheless, even the ability to transmit qubits in this imperfect way makes possible important protocols, such as end-to-end QKD, without reliance on trusted quantum repeaters.<sup>12</sup>

Figure 1. Quantum Key Distribution





Colonel Timothy Lawrence, director of Air Force Research Laboratory (AFRL)'s Information Directorate, speaks during virtual Million Dollar International Quantum U Tech Accelerator event, September 1–3, 2020, in Rome, New York, where AFRL's Air Force Office of Scientific Research later awarded 17 quantum information science grants (U.S. Air Force)

The prepare-and-measure stage requires DOD to realize the limitations of quantum transmission and the investment necessary to ensure a secure quantum Internet. The United States is falling behind China in efforts to capitalize on quantum technology, placing China on a path to achieve initial success in the realm of a quantum Internet, quantum communications, and quantum sensing. China is investing in its quantum military efforts, already claiming success in qubit transmission among Shanghai, Beijing, and other cities, via a land network of approximately 750 miles.<sup>13</sup> Although this achievement does not specifically indicate a successful demonstration of a quantum Internet, it does highlight that China is making gains while DOD and the U.S. Government are focusing primarily on quantum computing developments that

do not fully advance the infrastructure necessary for a quantum Internet.

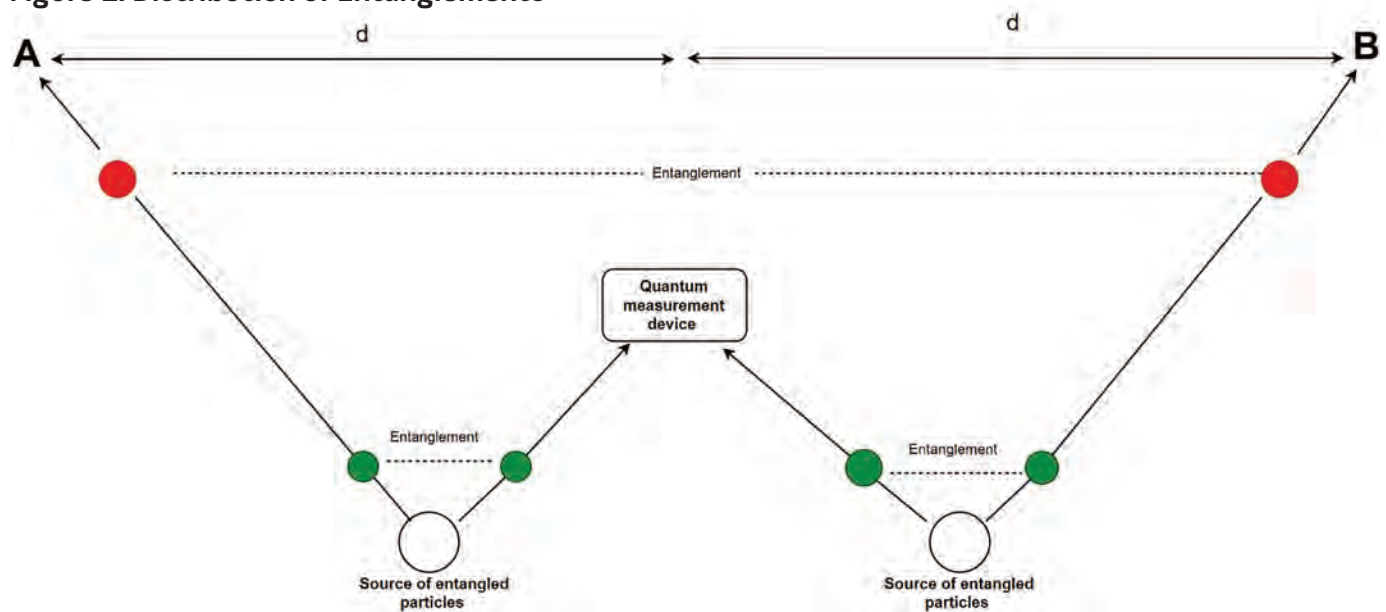
This second stage further establishes the principles of quantum sensing and its utility on the battlefield, as tactical surprise can set the stage for success in military operations. The concept of quantum sensing in this stage is possible when assessing perturbations in the quantum state. A quantum radar, such as the one Jonathan Baugh is developing at the University of Waterloo, in Canada, measures quantum states in a microwave beam and looks for anomalies in those states.<sup>14</sup> In military usage, the precision in quantum measurements would allow immediate and specific detection of combat assets, including problematic examples such as a stealth fighter or a submarine. The first military to develop such a radar will increase the effectiveness of its early-warning and target acquisition; therefore, the United

States must reach quantum supremacy before its adversaries do.

### Entanglement Generation Stage

At the third stage of development, the Internet can generate a pair of maximally entangled qubits and distribute them—one to node A and another to node B. This process must succeed with nearly unit probability. This stage bypasses the postselection requirement of the previous stage and enables a greater variety of protocols to be carried out between node A and node B. This stage could be implemented using true quantum repeaters, which function by receiving a qubit, entangling it with another, and passing the second qubit along (see figure 2). This “daisy chain” of entangled qubits results in the distribution of entanglement between the initial and final nodes of the chain.<sup>15</sup>

**Figure 2. Distribution of Entanglements**



Successfully distributed entangled qubits allow nodes to transmit qubits securely using a process called *quantum teleportation*. In addition, new and more secure forms of QKD could now be carried out between the end nodes, and the security of these new QKD protocols would no longer require end users to trust even their own measurement devices,<sup>16</sup> increasing their security.

At this stage, DOD could start to realize instantaneous communication regardless of the capacity of data flow, a critical component to promote military superiority via a more coordinated and immediate information environment. Dominance in the operational environment centers on forces, weapons, and systems that can maneuver, react, defend, and destroy at the time and space of a commander's choosing—and the surety of communications systems. At the entanglement generation stage, commanders have access to end nodes that allow secure and nearly instant transmissions, providing an edge to their forces with immediate synchronization of effort; this is especially true when simultaneous nonkinetic and kinetic effects are required to achieve a particular objective, as timing becomes critical through exercising instantaneous, uninterrupted communication. These issues showcase the urgency of

investment and research in achieving a capable quantum Internet.

### Quantum-Memory Stage

The next stage is crucial for a large quantum network to be possible. The main difference between this stage and the previous one is that at this newer stage multiple qubits can move from one network node to another. Quantum memory allows for a network to be established one state at a time, storing the quantum states as they are received from the network. This approach makes sending larger quantum states by quantum teleportation possible, which increases the volume of quantum information that can be transmitted. Moreover, at this stage, quantum clock synchronization and quantum anonymous transmission become feasible via a multiparty entanglement system.<sup>17</sup> Entanglement and quantum communication ensure that time signatures across multiple parties are authentic, improving the security of communication transmissions.<sup>18</sup>

The military would benefit from an advancement at this stage through more precision in clock synchronization, maximizing its ability to further achieve simultaneous operations during large-scale conflicts beyond what is accessible with the previous stage's communication gains.

Clock synchronization translates into exactness in both time alignment and GPS fidelity—crucial components for achieving military objectives in both time and space. The Defense Advanced Research Projects Agency notes the potential for improvement with quantum synchronization, which could increase efficiency from a billionth to a trillionth of a second.<sup>19</sup> This gain may seem inconsequential, but any increase in accuracy could mean the difference between success and defeat on the battlefield. Major Matthew Myer highlights this point well from an infantry perspective. As ground troops rely on air platforms to defeat the enemy in close missions—missions that may create incidents of fratricide due to the proximity of enemy and friendly forces—pilots must often change tactics and weapons systems to accommodate.<sup>20</sup> Every individual relying on lifesaving measures or the availability of a weapons system appreciates any increase in accuracy and timeliness.

### Few-Qubit Fault-Tolerant Stage

A fault-tolerant design enables a system to continue its intended operations, possibly at a reduced level, rather than failing completely when only some part of a system breaks. The term *few qubits* here refers to the fact that the number of qubits available is still small enough that the end nodes themselves could

be simulated on a classical computer.<sup>21</sup> Nevertheless, a classical computer may be unable to simulate the entire network. Reliable qubits are difficult to engineer, but standard fault-tolerance schemes exist that use seven or more physical qubits to encode each logical qubit, with still more qubits required for error correction.<sup>22</sup> The large overhead makes testing fault-tolerance schemes with multiple encoded qubits difficult. Access to fault-tolerant gates makes possible more accurate clock synchronization as well as distributed

quantum computing—that is, a network of quantum computers interconnected by quantum and classical channels. Because quantum computers are interconnected by quantum channels, users could leverage the entanglement required to obtain an increase of computational power. Moreover, small quantum computers linked by quantum connections could be a stepping-stone to future large-scale quantum computers. Even in this limited scenario, it might be feasible for users to perform computations at speeds not currently

possible with quantum computers, as researchers working on Google’s machines recently demonstrated.<sup>23</sup>

A fault-tolerant design could provide DOD with a viable quantum network on which it could rely in a satellite-denied environment, so that forces could continue to execute operations despite any adversary’s effort to defeat the military’s satellite connectivity. The Pentagon realizes this scenario as a realistic vulnerability and understands the benefits that quantum provides in overcoming it; however, DOD’s investment in maturing



Marine with Charlie Company, 8<sup>th</sup> Communication Battalion, conducts radio communication check during Exercise Cyber Fury 21, at Camp Lejeune, North Carolina, July 26, 2021 (U.S. Marine Corps/Armando Elizalde)

this technology is only a fraction of the budget China, another quantum giant, has dedicated to quantum development.<sup>24</sup> Therefore, to realize this stage and achieve a fault-tolerant design durable enough to survive the brutal conditions on the front lines of combat, DOD must continue to promote expertise in quantum computing and networking through initiatives such as the Million Dollar International Quantum U Tech Accelerator, a Navy and Air Force event that reviews pitches from experts competing for contracts to develop future quantum capabilities for DOD, while also promoting collaboration, innovation, and training in these technologies.<sup>25</sup>

### Quantum Computing Stage

This ultimate stage allows for the realization of all protocols. These protocols, among many others, would deliver secure communication, secure login networks, quantum-enhanced GPS, secure voting, quantum digital signature, gravitational wave detection, and so forth. But having a full-fledged quantum computer at the end of each node has both advantages and risks. One of the main risks is the breaking of cryptography as it currently exists. Shor's algorithm solves the discrete logarithm problem by using a quantum computer to factor a large integer.<sup>26</sup> With the advent of such quantum algorithms, as well as quantum

computers, and a quantum Internet, an adversary could efficiently break the universally adopted public key cryptosystem schemes (for example, RSA, DSA [digital signature algorithm], and ECC [elliptic-curve cryptography]) that rely on the computational difficulty of such factoring problems.

If DOD achieves the quantum computing stage first, it could take advantage of each of the previous stages while also having access to a system of quantum computers that could provide the level of analysis commanders need to succeed in any operational environment. A full-fledged quantum Internet means immediate access to quantum systems across



U.S. Cyber Command Cyber National Mission Force members participate in training and readiness exercise at Fort George G. Meade, Maryland, May 24, 2021 (U.S. Army/Josel Cole)

the Internet, thus offering immense computing power to analyze all possible data points that commanders have available to aid in the decision cycle. A quantum computer could pinpoint the best possible solution faster than could any classic computer. Moreover, the potential problem sets quantum computers can solve are still unfathomable, which means the power of these computers to aid on the battlefield, in real time, could change the character of war in ways we still do not understand. However, the success of the U.S. Armed Forces in the quantum environment is possible only if DOD elects to invest in the quantum Internet now.

DOD and other stakeholders should regard the development of the quantum Internet as a process that will occur over several stages, rather than as a single entity that will appear once quantum computing becomes feasible. By tracking and analyzing how the quantum Internet develops stage by stage, DOD could remain in step with technological advances of state and private actors and thus be better prepared for the eventual emergence of quantum computing. Conversely, ignoring this development and only countering the eventual emergence of a quantum computer, by investing in postquantum technologies, would put DOD at a disadvantage compared with other state and private actors. JFQ

## Notes

<sup>1</sup> Richard P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics* 21, nos. 6/7 (June 1982), 467–488.

<sup>2</sup> Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings: The 35th Annual Symposium on Foundations of Computer Science* (Washington, DC: Institute of Electrical and Electronics Engineers, 1994), 124–134.

<sup>3</sup> "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms," National Institute of Standards and Technology Call for Proposals, December 20, 2016, available at <<https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms>>.

<sup>4</sup> Stephanie Wehner, David Elkouss, and Ronald Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science* 362,

no. 6412 (2018), available at <<https://science.sciencemag.org/content/362/6412/eaam9288.full>>.

<sup>5</sup> Joint Publication 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), IV-6.

<sup>6</sup> Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (Cambridge, UK: Cambridge University Press, 2000).

<sup>7</sup> Richard Jozsa et al., "Quantum Clock Synchronization Based on Shared Prior Entanglement," *Physical Review Letters* 85, no. 9 (August 2000), 2010–2013, available at <<https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.2010>>.

<sup>8</sup> Wehner, Elkouss, and Hanson, "Quantum Internet."

<sup>9</sup> Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theoretical Computer Science* 560 (2014), 7–11. Originally published as Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *International Conference on Computers, Systems & Signal Processing*, vol. 1 of 3 (Bangalore, India: Institute of Electrical and Electronics Engineers, December 1984), 175–179, available at <<https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>>.

<sup>10</sup> Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus, "The Case for Quantum Key Distribution," in *Quantum Communication and Quantum Networking*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 36, ed. Alexander Sergienko, Saverio Pascazio, and Paolo Villoresi (Heidelberg, Germany: Springer, 2010).

<sup>11</sup> Nielsen and Chuang, *Quantum Computation and Quantum Information*.

<sup>12</sup> Charles H. Bennett and Stephen J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," *Physical Review Letters* 69, no. 20 (November 1992), 2881–2884.

<sup>13</sup> Tom Stefanick, "The State of U.S.-China Quantum Data Security Competition," *Brookings*, September 18, 2020, available at <<https://www.brookings.edu/techstream/the-state-of-u-s-china-quantum-data-security-competition/>>.

<sup>14</sup> Martin Giles, "The U.S. and China Are in a Quantum Arms Race That Will Transform Warfare," *MIT Technology Review*, January 3, 2019, available at <<https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/>>.

<sup>15</sup> Nicolas Sangouard et al., "Quantum Repeaters Based on Atomic Ensembles and Linear Optics," *Reviews of Modern Physics* 83, no. 1 (2011), 33–80.

<sup>16</sup> Umesh Vazirani and Thomas Vidick, "Erratum: Fully Device-Independent Quantum Key Distribution," *Physical Review Letters* 116, no. 8 (February 2016).

<sup>17</sup> Jozsa et al., "Quantum Clock Synchronization."

<sup>18</sup> Howard Barnum et al., "Authentication of Quantum Messages," in *Proceedings: The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002* (Washington, DC: Institute of Electrical and Electronics Engineers, 2002), 449–458.

<sup>19</sup> *Quantum Sensing and Computing: Advancing National Security Through Fundamental Research* (Washington, DC: Defense Advanced Research Projects Agency, n.d.), 2, available at <<https://www.darpa.mil/attachments/QuantumSensingLayout2.pdf>>.

<sup>20</sup> Matthew R. Myer, "Danger Close: Calculating Risk Within the 'Last 100 Yards,'" *Infantry Online*, 2013, available at <<https://www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html>>.

<sup>21</sup> Maarten Van den Nest, "Classical Simulation of Quantum Computation, the Gottesman-Knill Theorem, and Slightly Beyond," *Quantum Information & Computation* 10, no. 3 (March 2010), 258–271.


<sup>22</sup> Peter W. Shor, "Scheme for Reducing Decoherence in Quantum Computer Memory," *Physical Review A* 52, no. 4 (October 1995), R2493–R2496, available at <[https://www.cs.miami.edu/home/burt/learning/Csc670.052/pR2493\\_1.pdf](https://www.cs.miami.edu/home/burt/learning/Csc670.052/pR2493_1.pdf)>.

<sup>23</sup> Frank Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature* 574 (2019), 505–510, available at <<https://doi.org/10.1038/s41586-019-1666-5>>.

<sup>24</sup> Jon Harper, "Pentagon Trying to Manage Quantum Science Hype," *National Defense*, December 10, 2020, available at <<https://www.nationaldefensemagazine.org/articles/2020/12/10/pentagon-trying-to-manage-quantum-science-hype>>.

<sup>25</sup> Ibid.

<sup>26</sup> Shor, "Algorithms for Quantum Computation," 124–134.



Soldiers assigned to 1<sup>st</sup> Squadron, 152<sup>nd</sup> Cavalry Regiment, 76<sup>th</sup> Infantry Brigade Combat Team, 38<sup>th</sup> Infantry Division, Indiana Army National Guard, engage in Military Operations in Urban Terrain drill at Lešt military training center, Slovakia, November 10, 2019 (U.S. Air National Guard/Jonathan W. Padish)

# Fog of Warfare

## Broadening U.S. Military Use-of-Force Training for Security Cooperation

By Patrick Paterson

The United States uses its Armed Forces almost exclusively overseas, normally as part of a coalition operation but also for noncombat operations such as disaster relief and

---

Dr. Patrick Paterson is a Professor in the William J. Perry Center at the National Defense University. His most recent book, *The Blurred Battlefield* (JSOU Press, 2021), addresses the need for hybrid doctrines on the use of force for Latin American militaries combating violent crime groups.

security assistance. In overseas operations where an armed conflict is occurring, use-of-force rules are governed by the Geneva Conventions and other law of armed conflict (LOAC) treaties. However, in over 80 percent of countries in the world today, violence is being caused not by conventional state-on-state armed conflicts but rather by criminal activity—which is often as intense and violent as conventional conflicts between nations.<sup>1</sup> In these

conditions, LOAC does not apply; there is no *armed conflict* per the legal definition of the term. However, these low-intensity conflicts can be so violent that the militaries in many countries have been called to support police efforts. When U.S. military forces provide security assistance to partner nations in these circumstances, they are operating in a gray area that requires legal and operational knowledge of both military and police tactics.



This dichotomy—U.S. forces adhering to LOAC while international partners follow criminal law and human rights law—creates operational and legal difficulties during U.S. security assistance efforts, a multibillion-dollar program to train and equip U.S. military partners. Hence, when U.S. forces conduct training with other military forces, American forces might be working off one legal framework while partners are governed by another set of rules, ones that are much more restrictive regarding the use of force. Moreover, if U.S. personnel train allied forces on the laws of war in lieu of more restrictive criminal law techniques, those forces might then use inappropriate tactics, which could result in instances of excessive force or human rights violations.

This article examines the nature of contemporary conflicts from two perspectives: the legal references that guide operations and the rules on the use of force. It describes the key differences between military and police tactics on the use of force. These contrasts are particularly important for security assistance efforts that U.S. forces conduct with dozens of partner nations each year. For legal and operational alignment with its partners, the United States should broaden its doctrine and revise its policy on the use of force during security cooperation activities to include police tactics governed by criminal and human rights law.

### **Contemporary Warfare: Drifting Away from Conventional Conflict**

Since the end of the Cold War, the nature of conflicts has changed dramatically. State-on-state wars are rare.<sup>2</sup> As of mid-2020, fewer than a dozen countries (out of nearly 200 worldwide) were in a conflict with another nation. In about two dozen other countries, government security forces are combating organized armed groups.<sup>3</sup> In these cases, the levels of intensity and organization of these groups have crossed an operational threshold and permit government forces to use military firepower against them, according to international humanitarian law in the 1948 Geneva Conventions and 1977 Additional Protocols.

However, most countries have contemporary security challenges that fall below the threshold of an armed conflict and into the category of internal disturbances. The confrontations might be riots, violent crime waves, or gang and cartel violence that occur within the country's borders. Fighting internal to a state—such as violent drug cartels in Mexico, election violence in Kenya, dangerous gangs in El Salvador, or terrorists in France—could involve the military because of the number, violence, and armament of the adversary.<sup>4</sup> But these disputes do not reach a level of violence and organization common in armed conflicts and, therefore, are guided by law enforcement rules and human rights law, not the laws of war. Military forces conducting law enforcement are expected to use police tactics and procedures.

The Western Hemisphere is a good example of how security forces have had to adjust their use-of-force doctrine for contemporary conflicts. Of the nearly three dozen nations that make up Latin America and the Caribbean (to include Mexico), only one—Colombia—is fighting an armed conflict. Nearly all the other nations in the region, though, have had to deploy their militaries internally to support—or, in some cases, supplant—their police forces because of high levels of violence and crime.

Using military forces against armed criminal elements represents the gray zone of contemporary conflict, a blurred battlefield with significant operational and legal challenges. Under these circumstances, modern warfare is more like police work than encounters between military forces.<sup>5</sup> The opponents often consist of irregular forces that blend into the population rather than a conventional force that is easily distinguishable from civilians, such as wearing identifying insignia and openly carrying arms.<sup>6</sup> In many cases, the adversary is a group of well-armed criminals who use violence to profit from their illicit activities. Frequently, individuals in the community participate in the criminal economy to make money (as lookouts, informants, drug lab workers, and drivers, for example) but are not armed and should not be considered a direct threat to security forces.

At the same time, because of the proliferation of small arms in many countries, legitimate members of the community might be armed for self-protection or as part of a neighborhood watch organization or a local militia. In other words, an individual with a weapon should not automatically be considered a threat. In these cases, it is difficult to determine who is an armed criminal and who is a member of local law enforcement. Additionally, in contemporary low-intensity conflicts, the frontlines of the battlefield are constantly shifting and often indistinguishable, blurring the lines between the combatants and noncombatants. In urban settings, military firepower (such as artillery, mortars, heavy weapons, and air support) presents serious risk to the civilian population, and its use might be restricted by military leaders, elevating the danger for security forces. For these reasons, contemporary security operations require a mix of law enforcement skills very different from conventional military training. Domestic law enforcement operations require a vast amount of discretion, diplomacy, and discipline. Lethal force should be considered the recourse of last resort.<sup>7</sup>

### **Differences Between Military and Police Doctrine on the Use of Force**

LOAC and criminal law share several similarities. The right to life is paramount in both cases. Civilians are expected to be protected, property damage should be minimized, torture or cruel treatment is prohibited, prisoners and detainees have certain rights, and medical aid should be rendered to victims immediately. Fundamentally, both fields of law protect the rights of human beings and their property.

There are also significant differences between LOAC and criminal law. Militaries use overwhelming firepower to crush the fighting spirit or warfighting capacity of an opposing force. LOAC rules are much more permissive regarding the use of force. One scholar describes LOAC as a “predilection for violence.”<sup>8</sup> Or, as the International

Committee of the Red Cross puts it, the “conduct of hostilities paradigm tolerates more incidental loss of life than the law enforcement paradigm.”<sup>9</sup> In contrast, under criminal law, use-of-force rules are much more restrictive.

Under LOAC rules, once an opponent is declared an enemy combatant, he or she could be targeted immediately until considered *hors de combat*.<sup>10</sup> There is no requirement to capture or arrest, neither is there a requirement for escalation of force tactics. Lethal force could be used as a first resort. Captured or disabled enemies, however, are entitled to certain protections and rights. They must be treated humanely, given medical

attention if required, and held in safe and sanitary conditions, among other requirements. But they are not necessarily entitled to due process, a speedy trial, or legal representation. They are normally detained until the end of the conflict, when they are repatriated.

In contrast, under criminal law, the suspect could be targeted only if he or she is posing a significant threat of death or serious injury. Lethal force should be considered the last resort, and only a “clear and imminent threat” justifies deadly force. Law enforcement officers are required to attempt to detain the suspect before using lethal force—that is, capture, not kill. If circumstances

permit, police officers are obliged to give a clear warning of their intent to use force with sufficient time for the warning to be observed before resorting to lethal force. Police should also use escalation of force tactics and crisis intervention techniques before resorting to more aggressive actions. According to criminal and human rights law, detained suspects are entitled to certain civil and political rights: due process, to be informed of their rights, the right to counsel or a lawyer, the right to a fair trial, and presumption of innocence, among others. They cannot be held arbitrarily or for an excessive amount of time without trial.<sup>11</sup>



Romanian and Ukrainian special forces and U.S. Army Green Berets conduct close quarters battle training during U.S. Special Operations Command Europe's annual exercise Trojan Footprint 21, in Romania, May 6, 2021 (Courtesy Roxana Davidovits)

**Table 1. Typology of Conflicts Worldwide (2018)**

Type	International Armed Conflict	Non-International Armed Conflict	Other Situations of Violence
Description	State on State conflict	State vs. Organized Armed Group, a form of internal conflict	Internal disturbance that does not rise to the level of armed conflict
Currently Active?	7 involving 11 countries plus coalition of 14 nations fighting vs. Syria	51 in 23 countries	Approximately 165 countries
Percentage of All Countries	~ 5%	~ 12%	~ 83%

Sources: Annyssa Bellal, *The War Report: Armed Conflicts in 2018* (Geneva: Geneva Academy of International Humanitarian Law and Human Rights, 2019); Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook: Armaments, Disarmament and International Security* (Stockholm: SIPRI, 2019).

However, few militaries understand the differences between the two fields of law or how to distinguish between them operationally. One senior U.S. military legal expert describes partner-nation legal knowledge as “woefully inadequate.”<sup>12</sup> As a result, most foreign military forces are unprepared for the new nature of contemporary warfare. And since nearly all the military forces of U.S. foreign partners are operating internally to their country, they are required to apply human rights standards to protect the citizens of that country. It is critical that U.S. Servicemembers who frequently train and interact with U.S. allies understand the legal and tactical differences between the types of contemporary conflict.

Many countries may prefer that their armed forces use LOAC tactics to combat violent criminal groups. The military firepower provides an immense advantage to their security forces. However, the legal parameters require them to fight within the law enforcement paradigm. Combining the two fields of law as a hybrid doctrine is complicated. Governments in many countries have struggled to retrain their militaries and find a balance between military firepower and discretionary police tactics.

### U.S. Government Policy on the LOAC and Human Rights

The U.S. military operates in a fundamentally different way than most other countries. U.S. Armed Forces are legally prohibited from operating internally to the United States, except in extraordinary crises. U.S. military forces nearly always operate on foreign soil and prefer to rely nearly exclusively on LOAC

rules. At the same time, alliances and security cooperation efforts with partner nations are national priorities, ones that provide strategic advantages over potential adversaries. Three interrelated legal ideas account for how the U.S. military operates: complementarity, *lex specialis*, and extraterritoriality.

**Complementarity.** The first legal concept that explains U.S. use-of-force rules is *complementarity*. This term refers to the redundancy of protections for civilians that exists in both the LOAC and human rights law. Current U.S. policy contends that LOAC provides adequate human rights protection, so there is no need to apply both. According to U.S. policy, “compliance with the law of armed conflict will ensure compliance with human rights law.”<sup>13</sup> To some degree, that is accurate. A few prohibited actions exist within both LOAC and human rights law: torture, slavery, rape, depriving right to life, and discrimination, for example. However, the two fields of law also have significant differences, for example regarding targeting, use of lethal force, escalation of force tactics, and detention operations, that are much more restrictive under the law enforcement paradigm compared with under the armed conflict paradigm.

**Lex Specialis.** The second legal concept to understand is *lex specialis*: “the more specific rule overrides the more general rule.”<sup>14</sup> The Geneva Conventions and Additional Protocols contain an immense number of safeguards—nearly 400 provisions—for the protection of combatants, noncombatants, prisoners, and the wounded, among many other subjects. Under this concept and closely

related to extraterritoriality, the United States considers that any foreign military operations outside of its own territory involve only LOAC, not human rights law. While there are some areas of overlap, the LOAC and human rights law are separate and distinct bodies of law, according to U.S. military doctrine; one wholly replaces the other.<sup>15</sup> In fact, Department of Defense (DOD) policy states that “all members of the DOD comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations.”<sup>16</sup> Applying the laws of armed conflict during combat makes sense, but why would the same laws be applied, as DOD policy states, in “all other military operations,” if an armed conflict does not exist and the tensions can be resolved using police tactics?<sup>17</sup> Additionally, if armed Soldiers are forbidden on the streets of the United States because such actions represent an undue threat to civil and political liberties (per the Posse Comitatus Act), why would similar behavior be considered acceptable in other countries?

Until recently, *lex specialis* has been a widely accepted legal practice. However, with the evolution of conflict, the idea that LOAC could provide sufficient protection for human rights has come into question.<sup>18</sup> As several senior LOAC scholars acknowledge, “there is increasing overlap of human rights law and the law of armed conflict, particularly in non-international armed conflict.”<sup>19</sup> Under conditions on today’s blurred battlefields in which civilians and combatants blend, LOAC and human rights laws can no longer be distinctly and effectively separated.



U.S. Marine Raiders land outside small village during Military Operations in Urban Terrain rehearsals at Bright Star 21, September 11, 2021, in Mohamed Naguib Military Base, Egypt (U.S. Army/Dean Gannon)

Recent U.S. policy decisions on these issues indicate that changes are afoot. Several new legal precedents contend that human rights treaties continue to apply during armed conflicts and that, consequently, U.S. forces should consider both LOAC and human rights considerations simultaneously. The 2018 Judge Advocate General *Operational Law Handbook* states that “where LOAC is silent or its guidance inadequate, specific provisions of applicable human rights law may supplement or possibly even displace . . . the LOAC in a particular situation.”<sup>20</sup> In addition, the new *Commander’s Handbook on the Law of Land Warfare*, which was published jointly by the U.S.

Army and Marine Corps in August 2019 to replace the outdated 1956 *Law of Land Warfare Manual*, acknowledges that human rights continue to apply during armed conflict and that *lex specialis* may have limits in its applicability. The *Handbook* states, “a situation of armed conflict does not automatically suspend nor does LOAC automatically displace the application of all international human rights obligations.”<sup>21</sup>

*Extraterritoriality.* The third legal component of U.S. doctrine refers to the idea that military forces operating in other countries have obligations under human rights law in the territory that they occupy and in which they have

assumed de facto control of basic government functions. *Human rights are the protections citizens of a country have against their own government.* In that sense, according to U.S. policy, human rights are the responsibility of the local government, not of U.S. forces working overseas—unless the United States has explicitly assumed responsibility for the civil and political rights of that country.<sup>22</sup>

The U.S. position on extraterritoriality differs from that of the United Nations and many other countries that have ratified the International Covenant on Civil and Political Rights (ICCPR). The United States contends that the ICCPR does not oblige it to provide civil and political

**Table 2. Principal Differences Between LOAC and Human Rights Law**

Issue	Law of Armed Conflict	Human Rights Law
<b>Applicability</b>	Applies in international conflicts between nations or non-international internal conflicts against organized armed groups.	Applies in times of war or peace. Addresses the universal rights of citizens in their countries.
<b>Participants*</b>	Combatants, belligerents, insurgents, noncombatants, and civilians.	Fighters, criminals, and civilians.
<b>Principal References</b>	Geneva Conventions I–IV (1949) and Additional Protocols (1977).	Universal Declaration of Human Rights (1948); International Covenant on Civil and Political Rights; and International Covenant on Economic, Social and Cultural Rights.
<b>Institutional Oversight and Management</b>	International Committee of the Red Cross.	United Nations, particularly the Office of the High Commissioner of Human Rights.
<b>Main Issues</b>	Rights of combatants, noncombatants, wounded, prisoners, etc. More recent treaties include the use of chemicals, mines, biological, and laser weapons.	Political and economic rights, rights of women, children and people with disabilities, slavery, forced labor, racism, torture, and enforced disappearances.
<b>Principles Regarding the Use of Force</b>	Discrimination, humanity, necessity, proportionality, and precaution.	Legality, accountability, necessity, and proportionality.
<b>Violations</b>	Gross violations of LOAC are “war crimes.” “Crimes against humanity” and genocide can also occur during war.	Gross violations of human rights are “crimes against humanity” and can occur during times of war or peace.

\* In non-international armed conflicts, members of organized armed groups are not considered combatants and do not have combatant privileges.

guarantees to the citizens of an occupied nation because a state’s obligations under the ICCPR extend only to persons within its territory and subject to its jurisdiction.<sup>23</sup>

If, for the sake of academic discussion, LOAC does not provide sufficient protections of individuals’ human rights, then a military force operating in another country should be obliged to ensure its forces understand the distinctions between the laws of war and human rights law. In many ways, this makes sense. As one scholar put it, human rights laws cannot be dismissed so casually “as to allow a State party to perpetrate violations of [human rights] on the territory of another State, which it could not perpetrate on its own territory.”<sup>24</sup> The U.S. perspective on extraterritoriality is beginning to change. In 2014, the United States acknowledged that the Convention on Torture—one of the principal human rights treaties—continued to apply in times of armed conflict and could not be superseded by LOAC.<sup>25</sup>

### Rules on the Use of Force for U.S. Noncombat Operations

Broadening U.S. military training to include police tactics and operationalizing human rights would also have benefits for U.S. forces on noncombat assignments.<sup>26</sup> In addition to the overseas

deployments for combat operations, the United States frequently deploys forces for a variety of other military missions, including natural disaster responses and security cooperation efforts with partner nations.<sup>27</sup> Since 2001, an estimated 36 percent of U.S. deployments have been for noncombat events such as humanitarian assistance and disaster relief (HADR), noncombatant evacuation operations (NEO), or peacekeeping operations.<sup>28</sup> Under these conditions, sometimes called military operations other than war, there is no armed conflict; therefore, by definition, LOAC does not apply.<sup>29</sup>

For example, the United States conducted HADR missions in the southeastern Philippines in December 2012 following Typhoon Bopha; in Ukraine in August 2013 to assist with the investigation of downed Malaysian airliner MH17; again in the Philippines in November 2013 following Typhoon Haiyan, in Senegal and Liberia in 2014 in response to the Ebola crisis, in Haiti in October 2017 in the aftermath of Hurricane Matthew, in Peru in March 2017 in the wake of devastating floods, and in Dominica in September 2017 to evacuate American citizens after Hurricane Maria nearly completely destroyed the island.<sup>30</sup>

Since 2001, the United States has also conducted NEO to extract U.S.

Embassy personnel and their families from danger—in Côte d’Ivoire in September 2002, from Liberia and Mauritania in June 2003, from Haiti in February 2004, from Lebanon in 2006, and from South Sudan in 2016.<sup>31</sup> In addition to HADR and NEO deployments, U.S. forces have conducted a number of other noncombat missions, such as anti-poacher assistance to the Tanzanian Wildlife Management Authority in May 2018, water well construction in Caribbean nations, airlift assistance to Burundi, and a search-and-rescue mission to Uruguay. Hundreds of U.S. forces also deployed for training and to build partner capacity to Poland, Latvia, Romania, Ukraine, and other Eastern European nations as part of Operation *Atlantic Resolve*, designed to reassure Northern Atlantic Treaty Organization members considering Russian interferences.<sup>32</sup>

None of these operations involved an armed conflict, but little guidance on police tactics or criminal law was provided to deploying U.S. forces. In the absence of forcewide guidance, some military units developed their own internal doctrine to guide their forces. The rules on the use of force in these cases fall into criminal law as guided by human rights law. U.S. forces should be trained on police tactics and discretionary use-of-force rules rather than the “firepower-friendly”



U.S. Army paratroopers with 1<sup>st</sup> Battalion, 503<sup>rd</sup> Parachute Infantry Regiment, 173<sup>rd</sup> Airborne Brigade Combat Team, prepare to load onto C-130 Hercules aircraft at Lviv International Airport prior to multinational airborne jump alongside Polish paratroopers and Ukrainian paratroopers from 15<sup>th</sup> Battalion, 95<sup>th</sup> Air Assault Brigade, as part of Rapid Trident 2021, at International Peacekeeping Security Centre near Yavoriv, Ukraine, September 25, 2021 (U.S. Army/Hayden Hallman)

doctrine that applies during a conventional armed conflict. Sending U.S. forces into operations prepared for violent encounters when none exists could set dangerous expectations.

### Conclusion

The U.S. military is well trained in the law of armed conflict; however, most forces—particularly those assigned to security cooperation efforts with foreign partners—have little to no formal training in criminal law enforcement or human rights law. Military police and National Guard units are the exceptions. However, DOD regulations and manuals provide little guidance on criminal law or human rights law for most U.S. military general purpose forces.<sup>33</sup> As a result, few in the Armed Forces understand the differences among

LOAC, criminal, and human rights law or how to operationalize human rights for contemporary conflicts. When training and advising partner-nation forces, these legal gray areas place U.S. military units in a tenuous position; they may be tactically unprepared to advise partners on operations that fall below conventional armed conflicts.<sup>34</sup>

In partner nations that have assigned military personnel to law enforcement duties, Soldiers need extensive retraining to learn to fight an enemy that is mixed among the civilian population—situations that require a large amount of discipline, discretion, and caution. Soldiers without the proper training or education may commit operational errors that jeopardize their legitimacy among this population. For military forces unprepared for these types of operations and not equipped

with nonlethal weapons, there are few options between shouting and shooting. A young Soldier handed a rifle without training on escalation of force tactics or deescalation techniques may resort to lethal force too quickly when other effective nonlethal tactics are viable options.

As General H.R. McMaster writes, “Soldiers trained exclusively for conventional combat operations may be predisposed toward responding with all available firepower upon contact with the enemy. Such a reaction might result in the unnecessary loss of innocent life and run counter to the overall aim of operations.”<sup>35</sup> The Soldiers’ weaponry may also be inappropriate for the circumstances; a military rifle fires a higher velocity round, has much more energy, and can cause much more harm to civilians compared with standard police arms.

For these reasons, U.S. Servicemembers who frequently deploy to provide tactical training to military forces in other countries must understand the evolving nature of conflict and the rules on the use of force in contemporary warfare.

DOD should reexamine its doctrine considering the changing nature of conflict, the increased prevalence of noninternational armed conflicts, and the need to be legally and doctrinally aligned with its allies and partner nations. From the perspective of U.S. security cooperation programs, the requirement for an updated use-of-force doctrine is even more urgent because the United States frequently provides training and equipment to partners who operate in the law enforcement paradigm, not the conduct-of-hostilities paradigm. JFQ

---

## Notes

<sup>1</sup> Annyssa Bellal, *The War Report: Armed Conflicts in 2018* (Geneva: The Geneva Academy of International Humanitarian Law and Human Rights, April 2019), available at <<https://www.geneva-academy.ch/joomlatools-files/docman-files/The%20War%20Report%202018.pdf>>; Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2021: Armaments, Disarmament and International Security* (Oxford: Oxford University Press, 2021).

<sup>2</sup> See, for example, Bellal, *The War Report*; SIPRI, *SIPRI Yearbook 2021*.

<sup>3</sup> According to the Geneva Conventions, the two requirements of organized armed groups (OAG) in a non-international armed conflict are that the group's actions have reached "a minimum level of intensity and duration" and that the armed group "is organized and has the capacity to engage in military operations." Additional Protocol II sets an even higher threshold to be declared an OAG. It requires that the group be under a responsible command and exercise such control over a territory as to enable it to carry out sustained and concerted military operations. See *How Is the Term "Armed Conflict" Defined in International Humanitarian Law?* Opinion Paper (Geneva: International Committee of the Red Cross [ICRC], March 2008), 1.

<sup>4</sup> The ICRC refers to these internal disturbances as "other situations of violence." See the helpful ICRC document *Characteristics of Armed Conflicts & Other Situations of Violence* (Geneva: ICRC, October 2017), available at <[https://www.icrc.org/en/download/file/67234/handout\\_3\\_-](https://www.icrc.org/en/download/file/67234/handout_3_-)

[characteristics\\_of\\_armed\\_conflicts\\_other\\_situations\\_of\\_violence.pdf](#)>.

<sup>5</sup> See Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (London: Penguin Books, 2006), 16–17.

<sup>6</sup> A 2017 study ordered by the Chairman of the Joint Chiefs of Staff (CJCS) and managed by the Institute for National Strategy Studies at the National Defense University concluded that one of the principal causes for civilian casualties—despite significant operational effort to avoid harm to civilians—was the difficulty in identifying irregular forces in contemporary conflicts. See Patrick Paterson, *The Blurred Battlefield: The Perplexing Conflation of Humanitarian and Criminal Law in Contemporary Conflicts* (MacDill Air Force Base, FL: JSOU Press, 2021), 72–73, available at <[https://jsou.libguides.com/ld.php?content\\_id=60453868](https://jsou.libguides.com/ld.php?content_id=60453868)>.

<sup>7</sup> See Patrick Paterson, *Training Surrogate Forces in International Humanitarian Law: Lessons from Peru, Colombia, El Salvador, and Iraq* (MacDill Air Force Base, FL: JSOU Press, 2016), available at <[https://jsou.libguides.com/ld.php?content\\_id=24773901](https://jsou.libguides.com/ld.php?content_id=24773901)>.

<sup>8</sup> Naz K. Modirzadeh, "Folk International Law: 9/11 Lawyering and the Transformation of the Law of Armed Conflict to Human Rights Policy and Human Rights Law to War Governance," *Harvard National Security Journal* 5, no. 1 (2014), 236.

<sup>9</sup> *The Use of Force in Armed Conflicts: Interplay Between the Conduct of Hostilities and Law Enforcement Paradigms*, Expert Meeting Report (Geneva: ICRC, November 2013), 2.

<sup>10</sup> The definition of when an armed conflict occurs is simple: An (international) *armed conflict* exists when "one or more States have recourse to armed force against another State, regardless of the reasons or the intensity of the confrontation." If no armed conflict exists, then LOAC rules do not apply, and the crisis falls into the category of internal disturbances that are governed by criminal law and human rights law under the law enforcement paradigm. See ICRC, *How Is the Term "Armed Conflict" Defined in International Humanitarian Law?* and *The Manual on the Law of Non-International Armed Conflict, with Commentary* (Sanremo, Italy: International Institute of Humanitarian Law [IIHL], 2006).

<sup>11</sup> Portions of this summary are drawn from *To Serve and To Protect: Human Rights and Humanitarian Law for Police and Security Forces* (Geneva: ICRC, March 2014); United Nations (UN) General Assembly Resolution 34/169, *Code of Conduct for Law Enforcement Officials*, A/RES/34/169 (December 17, 1979), available at <<https://www.ohchr.org/Documents/ProfessionalInterest/codeofconduct.pdf>>; UN, *Basic Principles on the Use of Force and Firearms by Law Enforcement Officials*, available at <<https://www.ohchr.org/Documents/ProfessionalInterest/firearms.pdf>>; *Guiding Principles on Use of Force*

(Washington, DC: Police Executive Research Forum, 2016); *Seattle Police Department Manual*, NCJ Number 65002, March 1974, available at <<https://www.ojp.gov/pdffiles1/Digitization/65002NCJRS.pdf>>; and a number of other U.S. police manuals on the use of force.

<sup>12</sup> Senior U.S. military legal expert, phone interview with author, August 23, 2019.

<sup>13</sup> For an explanation of the complementarity policy in official Department of Defense (DOD) manuals, see Naval Warfare Publication 1-14M, *The Commander's Handbook on the Law of Naval Operations* (Norfolk, VA: Headquarters Department of the Navy, August 2017), 5-8. See also Army Field Manual (FM) 6-27/Marine Corps Tactical Publication 11-10C, *The Commander's Handbook on the Law of Land Warfare* (Washington, DC: Headquarters Department of the Army, September 2019), 1-26.

<sup>14</sup> *Lex specialis* signifies that whenever two or more norms deal with the same subject matter, priority should be given to the norm that is more specific. In other words, "the rule that is more specifically directed toward the action receives priority because it takes better account of the particular features of the context in which the law is to be applied, thus creating a more equitable result and better reflecting the intent of the authorities that have made the law." See *Department of Defense Law of War Manual* (Washington, DC: DOD, updated December 2016), para. 1.3.2.1, "The Law of War as the *Lex Specialis* Governing Armed Conflict," 9.

<sup>15</sup> See Dustin Kouba, ed., *Operational Law Handbook* (Charlottesville, VA: National Security Law Department, 2018), chap. 3, sec. V.A.1, 51.

<sup>16</sup> See DOD Directive 2311.01E, *DOD Law of War Program* (Washington, DC: DOD, May 9, 2006), para. 4.1. See also Human Rights Committee, "Observations of the United States of America on the Human Rights Committee's Draft General Comment 35: Article 9," June 10, 2014, para. 20, available at <<https://www.justsecurity.org/wp-content/uploads/2015/01/US-UN-HRC-GC-35.pdf>>. See also *Department of Defense Law of War Manual*, 9n13 and para. 17.2.1.3 (1018).

<sup>17</sup> DOD Directive 2311.01E, para. 4.1.

<sup>18</sup> During the International Court of Justice 1996 advisory opinion on the "Legality of the Threat or Use of Nuclear Weapons," the Court declared that "the protection of the International Covenant on Civil and Political Rights does not cease in times of war."

<sup>19</sup> IIHL, *Manual on the Law of Non-International Armed Conflict*, 15.

<sup>20</sup> *Operational Law Handbook*, chap. 3, sec. V.A.3, 52.

<sup>21</sup> See FM 6-27/MCTP 11-10C, para. 1-119, 1-26. To be clear, this is not a change to DOD policy regarding *lex specialis*, but it does represent an important acknowledgment that human rights continue to apply in situations of

armed conflict.

<sup>22</sup> There is extensive literature on legal rules for military forces acting as occupation forces. For more information, see Laurie R. Blank and Gregory P. Noone, “The Law of Belligerent Occupation,” in *International Law and Armed Conflict: Fundamental Principles and Contemporary Challenges in the Law of War* (New York: Wolters Kluwer Law and Business, 2013).

<sup>23</sup> See *Operational Law Handbook*, chap. 3, sect. II.D, 48–50.

<sup>24</sup> Dietrich Schindler, “Human Rights and Humanitarian Law: Interrelationships of the Laws,” *American University Law Review* 31 (1981–1982), 935, 941–942; Michael J. Dennis, “Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation,” *The American Journal of International Law* 99, no. 1 (January 2005), 119–120.

<sup>25</sup> Kenneth Watkin, *Fighting on the Legal Boundaries: Controlling the Use of Force in Contemporary Conflict* (New York: Oxford University Press, 2016), 149–150.

<sup>26</sup> This would require a change to current DOD policy, which is to apply LOAC to “all military operations.”

<sup>27</sup> For an informative infographic of U.S. military deployments, see Stephanie Savell, “Where We Fight: U.S. Counterterror War Locations,” *Costs of War* project (Providence, RI: Watson Institute for International and Public Affairs, January 2019), available at <<https://watson.brown.edu/costsofwar/papers/2019/where-we-fight-us-counterterror-war-locations-2017-2018>>.

<sup>28</sup> Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, September 17, 2006), identifies three major categories of military operations: major operations and campaigns; crisis response and limited contingency operations; and military engagement, security cooperation, and deterrence. The publication (V-2) also identifies 16 other types of operations. The author is indebted to William J. Perry Center Research Assistant Ana Cardona for collecting and assembling this information. Approximately 58 percent of U.S. deployments (measured by number of events, not number of personnel) involve counterterror operations or conventional conflicts such as those in Iraq, Afghanistan, Syria, Kosovo, and Bosnia-Herzegovina. For example, the United States had about 160,000 troops in Iraq at the war’s peak in 2005; 99,000 in Afghanistan in 2011, of which 83,000 worked under the International Security Assistance Force; 5,500 in Kosovo in 2001 working under the Kosovo Force; and 3,800 in 2001 in Bosnia-Herzegovina working for the Stabilization Force. Since 2001, U.S. forces—especially special operations forces—have conducted counterterror operations in Iraq, Afghanistan, Syria, Yemen, the Philippines, and Niger, among other nations.

All information on U.S. military deployments is drawn from Barbara Salazar Torreon and Sofia Plagakis, *Instances of Use of United States Armed Forces Abroad, 1798–2018*, R42738 (Washington, DC: Congressional Research Service, December 28, 2018).

<sup>29</sup> The U.S. Army defines *operations other than war* as “military activities during peacetime and conflict that do not necessarily involve armed clashes between two organized forces.” See FM 100-5, *Operations* (Washington, DC: Headquarters Department of the Army, June 14, 1993). The term *military operations other than war* was discontinued by Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, September 17, 2006).

<sup>30</sup> Between 1990 and 2000, the U.S. military responded to 61 humanitarian assistance and disaster response events. See the helpful list in Frank N. Schubert, *Other Than War: The American Military Experience and Operations in the Post-Cold War Decade* (Washington, DC: Joint History Office, 2013), 31–32.

<sup>31</sup> See the list of 18 noncombat evacuations conducted during the 1990s in *ibid.*, 33–34.

<sup>32</sup> *Ibid.*

<sup>33</sup> The standing rules for the use of force (SRUF) may be the closest example of guidance for U.S. Servicemembers conducting domestic law enforcement operations. Added to the most recent version of the standing rules of engagement (SROE) (CJCS Instruction 3121.01B, *Standing Rules for the Use of Force for U.S. Forces*, released June 13, 2005), the SRUF provide guidance for U.S. military personnel conducting domestic operations, particularly in Defense Support for Civil Authorities or homeland defense missions. Most of the SROE/SRUF are classified secret, but the *Domestic Operational Law: 2021 Handbook for Judge Advocates* (Charlottesville, VA: Center for Law and Military Operations, 2021) has a helpful description of the rules for the use of force for Federal forces in chap. 10, “Rules for the Use of Force (RUF) for Federal Forces,” 212.

<sup>34</sup> To see what training U.S. special operations forces provide to dozens of partnership forces each year, see *Foreign Military Training Joint Report to Congress* (Washington, DC: Department of State and DOD, various).

<sup>35</sup> H.R. McMaster, “Moral, Ethical, and Psychological Preparation of Soldiers and Units for Combat,” *Naval War College Review* 64, no. 1 (2011), 14–15.

## New from NDU Press

for the Center for the Study of Chinese Military Affairs

Strategic Forum 309  
*PLA Overseas Operations in 2035: Inching Toward a Global Combat Capability*

By Joel Wuthnow, Phillip C. Saunders, and Ian Burns McCaslin



The Chinese military presence in the “far seas” beyond Asia is growing and will expand further as

the PLA moves toward its 2035 goal of fielding a fully modern military. Existing overseas activities are mostly conducted by a single service and have not involved combat. Future scenarios for overseas joint operations include larger scale military operations other than war and overseas combat. Conducting more complex overseas operations would require substantial improvements in PLA capabilities, such as a stronger overseas joint logistics system. Changes in the domestic or regional security environment or intensified U.S.-China competition could accelerate a transition toward greater emphasis on expeditionary operations, including higher end combat scenarios.



Visit the NDU Press Web site for more information on publications at [ndupress.ndu.edu](http://ndupress.ndu.edu)





Rocket carrying last satellite of BeiDou Navigation Satellite System blasts off from Xichang Satellite Launch Center in southwest China's Sichuan Province, June 23, 2020 (Xinhua/Jiang Hongjing)

# BeiDou

## China's GPS Challenger Takes Its Place on the World Stage

By David H. Millner, Stephen Maksim, and Marissa Huhmann

Global navigation satellite systems (GNSS) provide a service many people take for granted. The GNSS applications people use fall into five major categories: location (determining a position), navigation (getting from one location to another), tracking

(monitoring movement of people or objects), mapping (creating maps of the world), and timing (calculating time). Generally, a GNSS has a constellation of at least 24 satellites in medium-Earth orbit (about 12,550 miles high) spread out around the world to deliver global

service.<sup>1</sup> Such GNSS capabilities are considered so essential that countries and alliances are simply unwilling to rely on each other for a system that is now considered indispensable to sovereignty. GNSS supports millions of applications that track and analyze our everyday lives—from farming, to finance, to reliable Internet. Simply put, it has become a vital service.

GNSS were created almost 50 years ago when U.S. scientists pioneered

---

Commander David H. Millner, USN, is the Senior U.S. Defense Official/Defense Attaché in Albania. Major Stephen Maksim, USSF, is Chief of the Engineering Liaison Office at the Air Force Nuclear Weapons Center. Lieutenant Commander Marissa Huhmann, USN, is currently serving as a Joint Expeditionary Public Affairs Officer in the Joint Planning Support Element under Joint Enabling Capabilities Command.



Marines with 1<sup>st</sup> Battalion, 25<sup>th</sup> Marine Regiment, navigate using Defense Advanced GPS Receiver while on patrol during exercise Northern Viper on Yausubetsu Training Area, Hokkaido, Japan, January 29, 2020 (U.S. Marine Corps/Jackson Dukes)

a global positioning system (GPS). Today, four countries operate GNSS: the United States has GPS, Russia has GLObal NAVigation Satellite System (GLONASS), the European Union (EU) has Galileo, and China has the BeiDou Navigation Satellite System, usually referred to as “BeiDou.” Japan and India have regional systems, and even the United Kingdom is planning for its own constellation since leaving the EU.<sup>2</sup>

With the launch of its final satellite to reach full system capability, China completed BeiDou in June 2020, and much has been made of the system and its features thus far.<sup>3</sup> But BeiDou is only the latest GNSS to come online since the United States developed GPS. Although much speculation and debate exist, it remains unclear if BeiDou will matter to the United States and other Western powers. An examination of the various types of GNSS reveals differences

in their development and military use/ adoption as well as in international response to them. This closer look sheds light on the likely impact of BeiDou, as it considers the system’s integration with China’s Belt and Road Initiative (BRI), the relationship with Russia and the EU, security concerns, and relative accuracy. A careful analysis of BeiDou and the multi-GNSS environment reveals that, although BeiDou does not represent a technological coup for the Chinese, it does constitute an incremental erosion of American technical prestige by presenting a viable alternative to GPS in an important sector that billions of people around the world use every day.

### GPS

GPS is the first and still predominant GNSS—so much so that using satellite navigation is synonymous with the initialism *GPS*. GPS was created in the

early 1970s, when the Department of Defense (DOD) wanted to guarantee a stable, accessible satellite navigation system for military use. DOD launched its first Navigation System with Timing and Ranging satellite in 1978; the 24-satellite system reached fully operational capability (FOC) in 1993.<sup>4</sup> DOD is constantly working to improve its satellites and the system; the latest block of GPS satellites, GPS III/IIIF, launched in 2018. These improvements help maintain GPS as the gold standard of GNSS.<sup>5</sup> As of June 2021, a total of 31 operational satellites were in orbit, including old and new satellites and on-orbit spares.<sup>6</sup> GPS currently delivers two levels of service: Standard Positioning Service, which is available to all users on a continuous, worldwide basis, free of any direct user charges; and Precise Positioning Service, whose access is restricted to the U.S. Armed Forces,

U.S. Federal agencies, and selected allied armed forces and governments.<sup>7</sup>

In the 1980s, President Ronald Reagan promised civilians they could gain access to GPS, but a feature called Selective Availability deliberately degraded location accuracy. This intentional degradation of GPS signals was meant to aid national security, as the feature allowed only “U.S. military and allies to access the second GPS signal for better accuracy.”<sup>8</sup> However, the Selective Availability policy increased the error for civil and commercial users by a considerable amount: 50 meters horizontally and 100 vertically.<sup>9</sup> Users became wary of U.S. intentions and ownership of GPS. In May 2000, President Bill Clinton signed a law discontinuing Selective Availability. Then, in 2007, DOD stated it would buy future satellites without the feature, and it has done so with the GPS III/IIIF satellites. Although this shift from Selective Availability has increased civil reliance on GPS, other countries nonetheless have moved forward with developing their own GNSS so as not to rely on the U.S. system.

GPS was developed by the U.S. military; however, the system boasts availability to users worldwide. The 2010 National Space Policy encouraged GPS- and GNSS-related international cooperation.<sup>10</sup> The policy directed the United States to “engage with foreign GNSS providers to encourage compatibility and interoperability, promote transparency in civil service provision, and enable market access for U.S. industry.”<sup>11</sup> The policy also states that the United States may use “foreign positioning, navigation, and timing (PNT) services . . . to augment and strengthen the resiliency of GPS.”<sup>12</sup>

## GLONASS

In keeping with its pattern of imitating U.S. technology, the Soviet Union decided to field its own GNSS. Development of GLONASS began in 1976, only 3 years after the United States started work on GPS.<sup>13</sup> GLONASS provides “real-time positioning and speed data for surface, sea, and airborne objects around the world.”<sup>14</sup>

The first generation of the GLONASS constellation was fully populated in 1996, but there was a gap in service between Kremlin governments: Only 7 of 24 satellites were still in operation in 2002, which hurt the system’s credibility.<sup>15</sup> Eager to regain its previous glory, the Russian Federation fully populated GLONASS, reaching FOC on December 8, 2011. The current generation once again features a constellation of 24 satellites. Active satellites boast longer design life, superior electronics, more capable radios, and sturdier hardware.<sup>16</sup> As in the case of GPS, military use and applications, such as precision-guided munitions, drove GLONASS requirements. GLONASS is an unabashedly military system, operated by the Russian Aerospace Defense Forces.<sup>17</sup> Because the system is global, the Russian military uses GLONASS in operations worldwide, such as recent actions in Syria.<sup>18</sup> Adoption of GLONASS was slow, even inside the Soviet Union and Russia.<sup>19</sup> However, Russia pushed international adoption around the time GLONASS regained full operational capability.

An agreement in 2000 allowed China not only to use GLONASS for basic navigation but also to field GLONASS-guided munitions.<sup>20</sup> Multiple sweeping agreements with China in 2019 include both the use of GLONASS (discussion of a previous GLONASS-BeiDou agreement follows later in this article) and interoperability with ground radar stations built to support BeiDou.<sup>21</sup> In 2008, Brazil signed up to use and help develop GLONASS as part of two major agreements on military technology.<sup>22</sup> In 2010, Russia signed an agreement to share the GLONASS high-precision signal with India.<sup>23</sup> Also in 2010, Ukraine signed an agreement with Russia to help develop GLONASS, after having agreed to help the EU establish Galileo just 5 years before.<sup>24</sup> Then, in 2013, Russia and Belarus signed a sweeping military and regulatory agreement that included GLONASS.<sup>25</sup> On the consumer front, Garmin and many cellphone manufacturers began supporting both GPS and GLONASS in 2011. These combined GPS/GLONASS multi-GNSS chipsets for cellphones and car navigation systems established the

design paradigm used by receivers in common use today that support GPS, GLONASS, Galileo, and BeiDou.<sup>26</sup>

## Galileo

Galileo is the European GNSS. The European Commission and European Space Agency built Galileo together to provide their member states with an independent, European alternative to GPS or GLONASS, as those systems can be degraded or denied by their owners at any time (though the United States has since pledged not to degrade GPS).<sup>27</sup> Galileo went live in 2016 and currently has 26 satellites in orbit; it will likely reach its goal of 30 satellites in the near future, as it recently suffered a launch delay.<sup>28</sup> Galileo currently provides all of its planned services, but performance will be enhanced when all satellites come online. Galileo delivers an open, free-to-the-public service and a more accurate Public Regulated Service that is restricted to military and emergency services.<sup>29</sup>

In contrast to its three “peer” services, which tout precision-guided munitions that use a secure signal, Galileo is a “kinder, gentler” system run by civilians instead of the military. Galileo has 28 partner nations, and its Public Regulated Service security modules must, by law, be produced in the EU to safeguard the hardware and software’s intellectual property. The regulated service requirements present obstacles to precision-guided munition manufacturers, which would need that information to implement Galileo-enabled guidance in their weapons.<sup>30</sup>

During the development of Galileo, significant tensions arose between the United States and the EU over the frequency of its Public Regulated Service. The EU had planned to use a frequency range that overlapped GPS’s military frequency. The frequency overlap would have prevented the United States from jamming Galileo’s high-precision service in a wartime scenario without also jamming an encrypted GPS frequency specific to the U.S. military. The United States also had serious concerns about China’s intentions to become a full member of the Galileo program. The EU eventually

agreed to alter the planned frequencies and terminate Chinese involvement.<sup>31</sup>

The EU cooperates with various intergovernmental organizations and nations around the world to promote Galileo and leverage it to help EU businesses.<sup>32</sup> Galileo has already been successful in receiving industry approval; in 2019, the technology to receive Galileo signals was incorporated into 1 billion cellular phones.<sup>33</sup> Given the historically cooperative nature of Galileo, as well as its minimal militarization, Galileo will likely provide the United States with beneficial augmentation to GPS.

## BeiDou

China decided to develop BeiDou after the 1995–1996 Taiwan Strait Crisis, when an unexpected disruption in GPS caused the People’s Liberation Army to lose track of its ballistic missiles fired over the Taiwan Strait.<sup>34</sup> China decided it could not afford to repeat such an incident and needed to invest in its own satellite-based PNT system.<sup>35</sup> Even though China had a standing agreement with Russia to use GLONASS for basic navigation and GLONASS-guided munitions, China persisted with its plan to develop BeiDou.<sup>36</sup> Given China’s emergence on the world stage and desire for recognition, this move is not surprising; Beijing desires a GNSS that it can maintain complete control of.

BeiDou is currently on its third generation of satellites. In 2000, BeiDou-1 was completed and began to provide PNT services to China only; in 2012, BeiDou-2 was completed and began to provide service to the Asia-Pacific region.<sup>37</sup> The third and final phase of the project, BeiDou-3, hit a milestone in 2018 when it began offering services globally. BeiDou-3’s preliminary system was completed with the launch of its final satellite in June 2020.<sup>38</sup> BeiDou uses two different general types of service: Radio Navigation Satellite Service (RNSS) and Radio Determination Satellite Service (RDSS). RNSS functions like other GNSS and was designed to have similar performance. RDSS is significantly different: A ground station using signals from the BeiDou satellites calculates a user’s position. The RDSS approach allows

for large-volume message communication and extended coverage.<sup>39</sup> However, any employment of BeiDou where ground stations are located allows the Chinese government to monitor a user’s location. Both RNSS and RDSS allow the user to send communications via short message service (SMS), a feature unique among the GNSS to BeiDou. The operational implications for such a feature mean that the Chinese government has a system to broadcast messages to any compatible BeiDou user in the world. The potential applications for such a feature are limitless.

Although every GNSS broadcasts a more accurate signal for only military and government use, BeiDou uniquely provides these sensitive users with information about the status and current accuracy of the navigation signal in real time.<sup>40</sup> BeiDou has been widely integrated with the Chinese military since at least 2014, and the military uses the SMS feature heavily; it is ideal for communicating among units and headquarters in remote locations. The military has also integrated BeiDou into its precision-guided munitions, including ballistic and cruise missiles.<sup>41</sup> Although China promotes BeiDou worldwide, especially within the Asia-Pacific region and BRI countries, its most developed BeiDou relationship is with Pakistan. As of December 2018, as part of a military cooperation agreement with China, Pakistan was the only country permitted to use the BeiDou restrictive service.<sup>42</sup> Pakistan also signed a first-of-its-kind agreement with China in 2013 to install five BeiDou ground augmentation stations and one processing center, allowing greater accuracy in the country.<sup>43</sup>

On July 9, 2019, the Consultative Assembly of Saudi Arabia agreed on a draft memorandum of understanding to cooperate on the military use of BeiDou. The Saudi Ministry of Defense and the Equipment Development Department of China’s Central Military Commission signed the memorandum. This agreement comes after the Second China-Arab States BeiDou Cooperation Forum, which took place April 1–2, 2020, in Tunis, Tunisia. Before this event, the two countries reportedly agreed in March 2019 to

“deepen military collaboration to jointly promote regional peace and stability.”<sup>44</sup>

China aggressively markets BeiDou to the private sector, especially as part of its BRI in Asian countries. In 2013, electronics leaders Qualcomm and Samsung collaborated to bring to market the first smartphones that included BeiDou; their smartphones and tablets were also the first to track three GNSS—GLONASS, GPS, and BeiDou.<sup>45</sup> Together, this marked an important milestone for inclusion of BeiDou in the world consumer electronics market as well as for the synthesis of multiple PNT systems on handheld devices. BeiDou made the transition to consumer electronics faster than did GLONASS, having entered the market at a later point in the maturity of handheld electronics after two other GNSS (GPS and GLONASS) had established demand and precedent. Smartphones began using Galileo in 2016, and it is now common for consumer devices to track using multiple GNSS.<sup>46</sup> Clearly, the consumer smart-electronics market saw value in utilizing other sources of PNT.

By the end of 2019, more than 70 percent of Chinese smartphones utilized BeiDou for positioning services—with a purported \$57 billion in goods and services tied to the capability. China aims to use BeiDou, together with its fifth-generation cellphone technology, to dominate the market for telecommunications services, which China envisions will include next-generation technologies such as autonomous vehicles. Agreements to use BeiDou under China’s expansive BRI have already been signed with 120 partners.<sup>47</sup> More than 30 countries, 400 million users, and 6.5 million vehicles use BeiDou.<sup>48</sup> Without abandoning GPS, thanks to multi-GNSS radio chipsets, the world has also embraced BeiDou.

## Comparisons

In addition to being a full-fledged GNSS, BeiDou is a critical piece in the digital architecture of China’s BRI. Consequently, China aggressively promotes BeiDou as part of its complete system of wares when it markets to other countries. China has indeed seen a surge

of activity regarding BeiDou within the international community in the past few years. Security professionals should anticipate more countries adopting the system or coordinating with China now that BeiDou has achieved FOC.

Somewhat surprisingly, Russia is one of those countries that, despite having GLONASS, signed a joint GLONASS-BeiDou cooperation and compatibility agreement in 2015. This agreement

was followed by a joint Chinese-Russian Silk Road Project that “marked the first, large-scale Sino-Russian effort to share, compare, and systematize satellite data” in 2017.<sup>49</sup> By 2018, China and Russia were able to agree on the same chipset, giving users “access to the total of GLONASS-BeiDou zone coverage, which spans across 40 functioning satellites” and “encompasses the Earth’s entire surface,” according to GLONASS

President Alexander Gurko.<sup>50</sup> This move created a technological interdependency between two countries that have long struggled to maintain a peaceful border.

As a GNSS, BeiDou offers a slight improvement over GLONASS in terms of accuracy and availability. When considered as an entire system with additional ground antennas, signal post-processing, and communications, BeiDou is superior to GPS, GLONASS, and Galileo. Time will tell if



Assembly of GLONASS-M spacecraft at JSC Academician M.F. Reshetnev Information Satellite Systems, Zheleznogorsk, Russia, January 12, 2015 (Yevgeny Kurskov/TASS/Alamy Live News)



Liftoff of Ariane 5 Flight VA240 from Europe's Spaceport in Kourou, French Guiana, on December 12, 2017, carrying Galileo satellites 19–22 (European Space Agency/Manuel Pedoussaut)

integration with the BRI makes BeiDou more—or less—appealing to the world.

China's relationship with the EU's Galileo is somewhat murkier. China's aborted participation in Galileo not only gave China BeiDou's technological underpinnings but also left it seemingly unencumbered by any fallout on the international scene. Comparing the military impact of Galileo and BeiDou directly is difficult because Galileo is civilian-run and not well-suited or marketed for weapons systems. Galileo is not part of a broad infrastructure initiative like BeiDou is with the BRI. The EU provides Galileo to the global community without significant installations in foreign territory or a political

agenda; it does not seem interested in marketing Galileo as a replacement for GPS but rather views Galileo as an augmentation or “kinder” alternative (per marketing). In the commercial domain, Galileo, much like BeiDou, has been widely accepted in the international marketplace for incorporation into both hardware and software applications. This level of incorporation will likely soften any political or economic impact from BeiDou on the United States simply by broadening the competition.

Unlike the Huawei 5G cellular network—another part of China's BRI that the U.S. Government is actively campaigning against in partner nations

due to security concerns—BeiDou does not pose an obvious security threat to users outside of Asia, where BeiDou ground stations are installed. Although concerns abound that the navigation signal may be able to install malware into a user's device, such possibility is highly unlikely, according to industry experts. However, malware could be installed through the BeiDou receiver chip, especially in a Chinese-manufactured device, or if the device uses the two-way transmission messaging service. Two-way transmission is necessary for BeiDou to monitor the location of the user and provide enhanced, post-processed position accuracy. Furthermore, most smartphone

manufacturers are not expected to utilize BeiDou's SMS functionality because the service requires a large amount of power and is not practical in a nondedicated device.<sup>51</sup> Thus, while many smartphones in the United States can already employ BeiDou as a GNSS, there is little security risk to U.S.-based users, as U.S. law does not allow the Chinese ground stations, which are required to track BeiDou users, to be installed in U.S. territory.<sup>52</sup> The traditional one-way listening activity of receiving PNT is inherently safe from a cyber-intrusion standpoint.

Demand for increased location accuracy—already a driving requirement—spurs innovation and competition in GNSS design. Measurements of accuracy depend heavily on the application and methodology. When solely relying on a real-time fix from orbiting satellites, all four GNSS have roughly comparable performance, given that GLONASS is closing the performance gap.<sup>53</sup> However, adding terrestrial antennas and signal post-processing, features that BeiDou is offering right now, promises orders of magnitude enhanced location accuracy that the physics of atmospheric and space flight prevent, thus enabling applications such as self-driving cars that the public yearns for.<sup>54</sup> The new capabilities will differentiate the next generation of GNSS.

## Analysis

The fielding of modern precision-guided munitions is the most obvious military implication of BeiDou, though China has had guided munitions with that capability for a long time—first through GPS and later through a diplomatic agreement with Russia. The completion of BeiDou does have some potentially positive aspects for the United States and other global competitors. BeiDou will provide redundancy for both civilian and military applications worldwide; most commercial technology now incorporates multiple GNSS to take advantage of that redundancy. This redundancy can have powerful advantages, like being able to receive more satellite signals while in an urban canyon or, while in open spaces, getting more accurate

positional data by using multiple GNSS. Militaries and governments worldwide can use BeiDou for redundancy as well. For example, American U-2 Dragon Lady pilots have been authorized to use multi-GNSS as a backup navigation system in case the aircraft's GPS fails.<sup>55</sup> Other U.S. military units could easily take advantage of BeiDou by incorporating similar commercial technologies into their toolkits. The United States should consider allowing the military to use multi-GNSS receivers produced by a trusted manufacturer.

Continued and diversified investment in space by other countries, especially peers and near-peers, reduces the strategic advantage of “nuking space,” whether literally or figuratively. Whereas in times past the overwhelming superiority and number of U.S. space-based platforms made the space domain itself a ripe target in a hot war, worldwide dependence on space, as well as the cost of repopulating constellations, acts as an incentive to preserve space as a global common.

Early on, the United States enjoyed a virtually unchallenged upper hand, as GPS was the gold standard of GNSS; this predominance made other nations dependent on the United States. That this reliance created tension in international relations is evident through the existence of now-multiple allied and adversary GNSS. When only GPS and GLONASS were available, countries worried about their reliance on just one or two systems. Now a solid quorum of GNSS gives all countries, both those with and without their own systems, a higher degree of confidence that they can plan on at least one system being available if another goes down.

Competition breeds innovation, though, and, even before BeiDou, GPS competed with both GLONASS and Galileo in a market that required constant improvements. That said, BeiDou may have applied new pressure. The newest GPS satellites (GPS III, which launched in 2018) will have three times better accuracy, up to eight times improved anti-jamming capabilities, and a longer lasting spacecraft.<sup>56</sup> With several global systems currently online, it behooves the U.S. militarily to ensure that GPS remains

the GNSS of choice. One addition in GPS III is a new signal that will “make it the first GPS satellite broadcasting a compatible signal with other international GNSS, like Galileo, improving connectivity for civilian users.”<sup>57</sup> Of course, innovation requires fresh capital. The U.S. military was projected to spend \$1.8 billion in fiscal year 2020 for GPS III, a figure that will likely increase as the United States contends with other GNSS.<sup>58</sup> The United States should focus on building the most reliable, accurate, and trusted source of PNT. Copying BeiDou's two-way communication method of delivering improved positioning accuracy at the cost of revealing user location and costly linear scalability is not a winning strategy in an expanding GNSS marketplace.

As worldwide reliance on GNSS expands, the criticality of these systems to multiple facets of modern life will continue to evolve; as a result, questions of sovereignty will loom as this critical infrastructure will hang, exposed, in the global commons of inner space. Tellingly, it was “desire for political sovereignty and control over a critical infrastructure” that sustained Galileo through years of strained planning and development. The United States should expect more nations to realize that depending on another's GNSS makes a country exactly that—dependent.<sup>59</sup> If China had decided to forgo pursuing a GNSS when the United States, EU, and Russian Federation had pursued theirs, such avoidance could have been interpreted as a sign of weakness or inferiority, especially in such a high “face culture.” After all, China considered the exposure of its dependence on GPS to be an “unforgettable humiliation.”<sup>60</sup> Because an emphasis on public image and a long societal memory are major aspects of Chinese culture, the United States should expect that China will attempt to never repeat this error.

## Conclusion

Examining other GNSS programs offers some unique insights into what the United States should expect with BeiDou. Comparing BeiDou with GLONASS and Galileo reveals that, although the Chinese system will not

cause a technological sea change in the GNSS ecosystem, BeiDou is significant and deserves attention, since it brings both security concerns and benefits to the United States. Through the lens of Great Power competition, BeiDou signifies another incremental erosion of the status of the United States as the sole superpower. China now offers sympathetic nations a viable GNSS alternative to GPS with highly competitive features that essentially did not exist before. Globally, GPS has been the de facto choice for PNT services because GLONASS was a markedly inferior service, and Galileo is only now coming into its own. BeiDou changes this status quo—it is clearly a better alternative than Galileo and GLONASS.

Despite GLONASS's rocky start, Russia was eventually successful in fielding its system and garnering international cooperation and use of its GNSS, including sharing GLONASS-enabled precision-guided munitions. Still, while Russia broke GPS's monopoly, it did not represent a fundamental shift in the status quo, neither was it an adequate replacement for GPS technologically. China has enormous economic, technological, and political advantages over Russia to speed the adoption of BeiDou as an (if not *the*) international standard of GNSS.

Galileo, set to reach FOC soon, may be aptly described as a demilitarized GPS without the political liability of single-country ownership. Galileo was quickly adopted by industry, and with multi-GNSS receivers already common, inclusion of BeiDou in most devices practically ensures that BeiDou will become the industry standard. It is, however, unlikely that BeiDou will displace GPS as the GNSS of choice for either military or civilian functions worldwide—BeiDou will likely become just another tool in the kit for most applications.

BeiDou does not pose a security threat for American users because the United States will not allow BeiDou ground stations in its territory; however, for nations participating in China's BRI and taking advantage of the additional capability that ground stations offer, security is a concern. These nations are

sacrificing privacy for access to superior service. Geopolitically, China has already sold access to its military-only signal to Pakistan and Saudi Arabia, allowing these countries to use BeiDou-enabled precision-guided munitions, which need not rely on other foreign GNSS, thus complicating any U.S. effort to deny these nations military-grade PNT capabilities directly through GPS.

BeiDou brings some benefits to the United States and the global community. Multi-GNSS receivers provide redundancy, additional features, and better positional accuracy, and BeiDou only deepens these advantages. Chinese investment in BeiDou also reduces the risk of conflict in the space domain, since physical destruction of any satellites puts other satellites in that orbit at risk, making kinetic conflict in space a shakier proposition. Finally, BeiDou forces all systems to innovate or risk becoming obsolete. The United States should take advantage of the benefits BeiDou provides while maintaining a vigilant eye on the security threats and implications that it brings. With the prestigious work of pioneering GPS complete, many other countries now join the United States in space, vying for dominance in navigation. The Nation would benefit from continued technological advances in GPS to keep it the gold standard of GNSS in this increasingly competitive field. JFQ

## Notes

<sup>1</sup> "How GPS Works," *GPS.gov*, n.d., available at <<https://www.gps.gov/multimedia/poster/>>.

<sup>2</sup> Callum Hoare, "UK Galileo Replacement to Integrate with U.S. GPS as Brexit Inspires 'New Relationship,'" *Express*, December 10, 2019, available at <<https://www.express.co.uk/news/uk/1215391/Brexit-news-uk-galileo-gnss-satellite-system-us-gps-chris-skidmore-eu-spt>>.

<sup>3</sup> Andrew Jones, "Final Beidou-3 Satellite Reaches Operational Orbit, China's Launch Sites Gear Up for July Missions," *Space News*, June 30, 2020, available at <<https://spacenews.com/final-beidou-3-satellite-reaches-operational-orbit-chinas-launch-sites-gear-up-for-july-missions/>>.

<sup>4</sup> National Aeronautics and Space Administration (NASA), "Global Positioning

System History," n.d., available at <[https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS\\_History.html](https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html)>.

<sup>5</sup> J. David Grossman, "The Path to a More Resilient and Robust GPS," *C4ISRNET*, April 22, 2021, available at <<https://www.c4isrnet.com/opinion/2021/04/22/the-path-to-a-more-resilient-and-robust-gps/>>.

<sup>6</sup> "Space Segment," *GPS.gov*, n.d., available at <<https://www.gps.gov/systems/gps/space/>>.

<sup>7</sup> NASA, "Global Positioning System History."

<sup>8</sup> GIS Geography, "Selective Availability in Global Positioning System (GPS)," n.d., available at <<https://gisgeography.com/selective-availability-gps/>>.

<sup>9</sup> Ibid.

<sup>10</sup> *National Space Policy of the United States of America* (Washington, DC: The White House, June 28, 2010), available at <[https://obamawhitehouse.archives.gov/sites/default/files/national\\_space\\_policy\\_6-28-10.pdf](https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf)>.

<sup>11</sup> "International Cooperation," *GPS.gov*, n.d., available at <<https://www.gps.gov/policy/cooperation/>>.

<sup>12</sup> *National Space Policy of the United States of America*.

<sup>13</sup> Richard B. Langley, "GLONASS: Past, Present and Future: An Alternative and Complement to GPS," *GPS World* 28, no. 11 (2017), 44–49, available at <<http://digital.gpsworld.com/publication/?m=59713&i=706479&p=49&pp=1&ver=html5>>.

<sup>14</sup> "Russian Armed Forces Use Glonass Satellites for Aiming in Syria," *GPS Daily*, May 17, 2016, available at <[https://www.gpsdaily.com/reports/Russian\\_Armed\\_Forces\\_Use\\_Glonass\\_Satellites\\_for\\_Aiming\\_in\\_Syria\\_999.html](https://www.gpsdaily.com/reports/Russian_Armed_Forces_Use_Glonass_Satellites_for_Aiming_in_Syria_999.html)>.

<sup>15</sup> Langley, "GLONASS: Past, Present and Future."

<sup>16</sup> Ibid.

<sup>17</sup> "Russia Launches One More Satellite to GLONASS Fleet," *Geospatial World*, May 30, 2016, available at <<https://www.geospatialworld.net/news/russia-adds-one-more-satellite-to-glonass-fleet/>>.

<sup>18</sup> "Russian Armed Forces Use Glonass Satellites for Aiming in Syria."

<sup>19</sup> Langley, "GLONASS: Past, Present and Future."

<sup>20</sup> B. Rivers, "PRC, Russia Close to GLONASS Agreement," *Journal of Electronic Defense*, 2000.

<sup>21</sup> See "Putin Approves Ratification of GLONASS, BeiDou Cooperation Agreement with China," *Russia & CIS General Newswire*, 2019; "Russia Will Be Able to Use 3 Chinese Ground Stations to Correct Satellite Signals—Roscosmos," *Russia & CIS General Newswire*, 2019.

<sup>22</sup> Imanuela Ionescu, "Brazil-Russia Military-Technical Cooperation: A Fruit of the Post-Cold War World Order," *Military Review* 98, no. 6 (2018), 66–79.



<sup>23</sup> “Russia, India Ink Agreement to Share GLONASS Signals,” *Mint*, December 21, 2010, available at <<https://www.livemint.com/Politics/kPdhPb6AOduzuZcSB8hjP/Russia-India-ink-agreement-to-share-GLONASS-signals.html>>.

<sup>24</sup> “Ukraine-Russia GLONASS Agreement,” *Ukraine General Newswire*, 2010.

<sup>25</sup> “Russia, Belarus to Cooperate in Using GLONASS Satellite Navigation System—Agreement,” *Russia & CIS Business and Financial Newswire*, 2013.

<sup>26</sup> Langley, “GLONASS: Past, Present and Future.”

<sup>27</sup> European Space Agency (ESA), “Why Europe Needs Galileo,” n.d., available at <[http://www.esa.int/Applications/Navigation/Galileo/Why\\_Europe\\_needs\\_Galileo](http://www.esa.int/Applications/Navigation/Galileo/Why_Europe_needs_Galileo)>.

<sup>28</sup> “Soyuz Launch from Kourou Postponed Until 2021, 2 Others to Proceed,” *Space Daily*, May 19, 2020, available at <[https://www.spacedaily.com/reports/Soyuz\\_launch\\_from\\_Kourou\\_postponed\\_until\\_2021\\_2\\_others\\_to\\_proceed\\_999.html](https://www.spacedaily.com/reports/Soyuz_launch_from_Kourou_postponed_until_2021_2_others_to_proceed_999.html)>; European Union Agency for the Space Programme (EUSPA), “Constellation Information,” available at <<https://www.gsc-europa.eu/system-service-status/constellation-information>>; ESA, “What Is Galileo?” n.d., available at <[http://www.esa.int/Applications/Navigation/Galileo/What\\_is\\_Galileo](http://www.esa.int/Applications/Navigation/Galileo/What_is_Galileo)>.

<sup>29</sup> EUSPA, “Services,” n.d., available at <<https://www.gsc-europa.eu/galileo/services>>; Jordan Wilson, *China’s Alternative to GPS and Its Implications for the United States*, Staff Research Report (Washington, DC: U.S.-China Economic and Security Review Commission, January 5, 2017), available at <<https://www.uscc.gov/research/chinas-alternative-gps-and-its-implications-united-states>>.

<sup>30</sup> Tim Vasen, “Is NATO Ready for Galileo?” *The Journal of the JAPCC* 28 (Spring/Summer 2019), available at <<https://www.japcc.org/is-nato-ready-for-galileo/>>. At the time of this publication, the author of this article was not aware of any precision-guided munitions designed to use Galileo’s Public Regulated Service, though it is likely they are being developed by European manufacturers.

<sup>31</sup> “EU, U.S. Split over Galileo M-Code Overlay,” *GPS World*, 2002.

<sup>32</sup> EUSPA, “International Co-operation,” n.d., available at <<https://www.gsa.europa.eu/galileo/international-co-operation>>.

<sup>33</sup> EUSPA, “Galileo Is the European Global Satellite-Based Navigation System,” updated September 16, 2021, available at <<https://www.euspa.europa.eu/european-space/galileo/What-Galileo>>.

<sup>34</sup> Minnie Chan, “Unforgettable Humiliation’ Led to Development of GPS Equivalent,” *South China Morning Post*, November 13, 2009, available at <<https://www.scmp.com/article/698161/>>

unforgettable-humiliation-led-development-gps-equivalent>.

<sup>35</sup> Ibid.

<sup>36</sup> Rivers, “PRC, Russia Close to GLONASS Agreement.”

<sup>37</sup> Rui Li et al., “Advances in BeiDou Navigation Satellite System (BDS) and Satellite Navigation Augmentation Technologies,” *Satellite Navigation* 1, no. 12 (2020), available at <<https://doi.org/10.1186/s43020-020-00010-2>>.

<sup>38</sup> Jones, “Final Beidou-3 Satellite Reaches Operational Orbit.”

<sup>39</sup> Rui C. Barbosa, “Chinese Bolster Navigation System with Dual Beidou Launch,” *NASA Spaceflight*, November 22, 2019, available at <<https://www.nasaspaceflight.com/2019/11/chinese-bolster-navigation-system-dual-BeiDou-launch/>>.

<sup>40</sup> Ajey Lele, “Space Security Dilemma: India and China,” *Astropolitics* 17, no. 1 (2019), 23–37, available at <[doi.org/10.1080/14777622.2019.1578932](https://doi.org/10.1080/14777622.2019.1578932)>.

<sup>41</sup> Kevin McCauley, “Putting Precision in Operations: Beidou Satellite Navigation System,” *China Brief* 14, no. 16 (August 22, 2014), available at <<https://jamestown.org/program/putting-precision-in-operations-beidou-satellite-navigation-system/>>.

<sup>42</sup> Maria Abi-Habib, “China’s ‘Belt and Road’ Plan in Pakistan Takes a Military Turn,” *New York Times*, December 19, 2018.

<sup>43</sup> Deng Xiaoci, “Pakistan 1<sup>st</sup> Foreign Nation to Fully Benefit from China’s BeiDou System,” *Global Times*, May 17, 2017.

<sup>44</sup> RWR Advisory Group, “Saudi Arabia Agrees to Cooperate in the Military Use of China’s Beidou Navigation Satellite System,” July 11, 2019, available at <<https://www.rwradvisory.com/saudi-arabia-agrees-to-cooperate-in-the-military-use-of-chinas-BeiDou-navigation-satellite-system/>>.

<sup>45</sup> “Qualcomm Collaborates with Samsung to Be First to Employ BeiDou for Location-Based Mobile Data,” *GPS World*, November 22, 2013, available at <<https://www.gpsworld.com/qualcomm-collaborates-with-samsung-to-be-first-to-employ-BeiDou-for-location-based-mobile-data/>>; David Manners, “Qualcomm, Samsung Add BeiDou to Glonass and GPS for More Precise Location Tracking,” *Electronics Weekly*, November 22, 2013, available at <<https://www.electronicweekly.com/news/business/finance/qsulcomm-samsung-add-BeiDou-to-glonass-and-gps-for-more-precise-location-tracking-2013-11/>>.

<sup>46</sup> “1 Billion Now Use Galileo Smartphones,” *GPS World*, September 10, 2019, available at <<https://www.gpsworld.com/1-billion-now-use-galileo-smartphones/>>.

<sup>47</sup> Jonathan Shieber, “China Nears Completion of Its GPS Competitor, Increasing the Potential for Internet Balkanization,” *Tech Crunch*, December 28, 2019, available at <<https://techcrunch.com/2019/12/28/china-nears-completion-of-its-gps-competitor->

increasing-the-potential-for-internet-balkanization/>.

<sup>48</sup> P.W. Singer and Taylor A. Lee, “China’s Version of GPS Is Almost Complete. Here’s What That Means,” *Popular Science*, March 31, 2020, available at <<https://www.popsci.com/story/blogs/eastern-arsenal/BeiDou-china-gps-gnss/>>.

<sup>49</sup> Mark Episkopos, “Is This the Real Russia-China Alliance America Should Fear?” *The National Interest*, December 16, 2018, available at <<https://nationalinterest.org/blog/buzz/real-russia-china-alliance-america-should-fear-38762>>.

<sup>50</sup> Ibid.

<sup>51</sup> Jim Mollenkopf, Senior Director, Strategic Development Qualcomm Government Technologies, interview with U.S.-China Economic and Security Review Commission staff, October 14, 2016; David Stelpstra, geodetic engineer, TomTom NV, interview with commission staff, October 14, 2016; Engineer, Qualcomm, Inc., interview with commission staff, August 19, 2016.

<sup>52</sup> Wilson, *China’s Alternative to GPS*.

<sup>53</sup> Alan Cameron, “K2 Will Drive GLONASS Under 1M,” *GPS World*, June 20, 2019, available at <<https://www.gpsworld.com/k2-will-drive-glonass-under-1m/>>; EUSPA, “Services”; Wilson, *China’s Alternative to GPS*; Lele, “Space Security Dilemma.”

<sup>54</sup> Wilson, *China’s Alternative to GPS*.

<sup>55</sup> Eric Tegler, “Why Are U-2 Jet Pilots Wearing Garmin Satellite Navigation Smartwatches?” *Ars Technica*, March 13, 2020, available at <<https://arstechnica.com/gadgets/2020/03/why-are-u-2-jet-pilots-wearing-garmin-satellite-navigation-smartwatches/>>.

<sup>56</sup> Alan Cameron, “Benefits Coming from GPS III Constellation,” *GPS World*, April 1, 2019, available at <<https://www.gpsworld.com/benefits-coming-from-gps-iii-constellation/>>.

<sup>57</sup> Lockheed Martin, “GPS III/IIIF: The Next Generation of Positioning, Navigation, and Timing,” available at <<https://www.lockheedmartin.com/en-us/products/gps.html>>.

<sup>58</sup> Stephen M. McCall and Brendan W. McGarry, “FY2020 National Security Space Budget Request: An Overview,” Congressional Research Service, June 7, 2019, available at <<https://fas.org/sgp/crs/natsec/IF11244.pdf>>.

<sup>59</sup> Ivan G. Petrovski, *GPS, GLONASS, Galileo, and BeiDou for Mobile Devices: From Instant to Precise Positioning* (Cambridge, UK: Cambridge University Press, 2014), xvii.

<sup>60</sup> Chan, “Unforgettable Humiliation.”



## An Interview with Richard D. Clarke

*JFQ: What are your priorities as commander of U.S. Special Operations Command [SOCOM]? Have these changed since you took command in 2019? If so, how and why?*

General Richard D. Clarke, USA, is Commander of U.S. Special Operations Command.

*General Clarke:* When I came into command, I had some thoughts about priorities and where to take the command, having just come from the Joint Staff. I was also given some great guidance from Secretary [James] Mattis who put me in the position. I sat down with all the commanders and

the senior enlisted leaders, and we set the priorities.

Those priorities have largely remained unchanged: compete and win for the Nation, preserve and grow readiness, innovate for future threats, advance partnerships, and strengthen our force and family. While I would argue that the operating environment has changed in those years—and it's now clear that China is our pacing threat—these priorities are timeless for SOCOM going into the future.

*JFQ: As you know, SOCOM has three Department-wide coordinating authority roles: countering violent extremist organizations [CVEO], countering weapons of mass destruction [CWMD], and the Internet-based military information support operations [MISO]. How do you see global security challenges affecting the ability of special operations forces [SOF] to perform these missions and your ability to stay ready and modernize?*

*General Clarke:* It's important first to talk about how coordinating authority is supposed to be executed and what a coordinating authority even is. The way I look at coordinating authority is that it is to lead planning, assess, and provide recommendations. And in that role, I provide those recommendations in those three areas you just brought up. But every Service and every combatant command is critical to helping address CWMD, CVEO, and Internet-based MISO—or WebOps. They all know the information space is important.

I think we can all agree that terrorism and violent extremism aren't going away. They're still threats. But we must approach countering these threats in a sustainable way because in the long run, they are not as important as the pacing threats or those near-peer threats we're seeing today with Russian activities in Ukraine.

For the CWMD threat, I think we should all be more concerned about where that is. On the nuclear basis, everyone's seen the buildup that China has undertaken with its nuclear capabilities. For the first time in our history, we're going to have two near-peer nuclear threats.

But then look at the chem-bio [chemical-biological] aspect. On the bio side, all you have to do is look at COVID-19 and what the pandemic has done to our nation. Then if you look on the chem side, the bar has been lowered on two fronts. One is the barrier to entry. Terrorists have used sarin and mustard gas in Syria and Iraq. And we know for a fact that the capability for terrorists to use chemical agents is there.

Then we've had state actors—like Kim Jong-un—using it against a family member. There have been several instances that prove the Russians have used it against political adversaries of the Russian government outside their own soil—in a U.S. Ally's territory. We all are sure that the landscape is changing and that we must in fact prepare the joint force for those possibilities.

Finally, the other important coordinating authority is WebOps or MISO. This is critical to campaigning in the gray zone because it's below the threshold of conflict. As everyone is aware, misinformation and disinformation are being sown by many of our competitors, and the problem is only growing. We have to be able to see that in real time. But we also have to be able to counter with all elements of statecraft.

I think we're seeing great examples of that today where we, as a government, are releasing intelligence to show malign behavior and are going public with it. And once it's been released publicly, it's then being reinforced in the information space by many. It's a great example of how information operations are going to remain critical going forward—as you look at integrated deterrence and

detering our adversaries. We've all studied deterrence theories, and it is as much in the mind of the person you're trying to affect. That is important.

*JFQ: Special operations are so heavily dependent on the quality of the people who carry out these missions. How are your units leveraging the diverse talents, skills, and backgrounds of your special operators and their partners while performing their missions?*

**General Clarke:** SOF truth number one: Humans are more important than hardware. We continuously come back to that. That fact will remain inviolable. We are going to continue to recruit and retain the best talent that our nation can provide.



Special operations forces from Cyprus, Greece, Serbia, and United States board Greek CH-47 Chinook during ORION 21, June 3, 2021 (U.S. Army/Monique O'Neill)



Special Warfare Combatant-Craft Crewman candidates from Basic Crewman Selection Class 111 low-crawl under obstacle during “The Tour” at Naval Special Warfare Center in Coronado, California, June 1, 2020 (U.S. Navy/Anthony W. Walker)

Today’s challenges continue to show that the number one SOF value proposition is our people. It’s the culture of who we are—our innovative problem-solvers. We’ve been emphasizing that they’re part of a cohesive and disciplined team that’s going to accomplish some of our nation’s hardest missions.

Those dedicated and trusted professionals are forward, fighting in combat zones, but also working with allies and partners. And they’re conducting the WebOps MISO. It’s emphasizing the whole of our force.

What we’re trying to do at all times is tap into our nation’s incredibly deep pool of talent. And we welcome anyone who wants to join our formation who is capable of meeting our standards—from all walks of life.

A lot of people think about SOCOM as just the military component. In addition to 70,000 Active-duty members, we also have 10,000 civilians who are part of this team. Some of them deploy with us,

but a lot of them are technical experts—whether it’s in acquisition, technology, or procurement of our special operations equipment. We have talented professionals throughout—to include our artificial intelligence and machine learning experts that are coding and helping us develop new capabilities across the board.

We’re going to recruit and retain a very diverse force with cultural and language expertise. Inherently, we are also a joint team. If you come to SOF, you know that we’re “born purple.” I’d say we integrate with the joint force at a lower echelon than any other force.

*JFQ: How do you see the special operators in relation to achieving the concept of jointness? What is the working relationship between your command and the Services that provide the capabilities you task? Do you see areas where the Services and National Guard might better leverage what special operators bring to the joint force?*

**General Clarke:** As I said a moment ago, many say that if you come into SOF, you are born purple. We inherently work as a joint team, and we bring joint and combined solutions at a lower echelon than any other part of our joint force. This was born out of Operation *Eagle Claw* with the failed rescue attempt [of American hostages in Iran] that brought about our modern-day SOCOM.

It also addresses the realities of our adversaries’ malign behavior because we must come together to see and understand. And we need to build access and placement to reach locations that small teams can access—but with a joint capability that can help solve those problems. Because our forces are inherently joint, they can reach back into the best of the Services and bring in those lessons learned and those experiences from both the SOF and the conventional sides of the force.

One thing that we must be aware of is that SOF can’t be the easy button or the solution to everything. There have been

times when it's just more convenient or easier to say, "Let's get SOF to do it." We have to stick with our core missions.

We shouldn't be put into a conventional-type fight when we're not the appropriate tool. Back in World War II, a Ranger battalion was completely wiped out in Italy because it wasn't properly employed. If we're not careful and observant, the same type of activities could take place today. We always have to be very cognizant of that.

*JFQ: As a combatant command with unique Title X authorities to develop a budget input for DOD [Department of Defense] and to direct spending, what has been your experience with Congress in advocating how you train and equip your force?*

**General Clarke:** We as a force are more integrated, credible, and capable than ever before and that really stems from the steadfast support of Congress. Congress established SOCOM in 1987. That was against the recommendations of the Chairman of the Joint Chiefs of Staff. As I discussed earlier, this was born from Operation *Eagle Claw* in 1980. Senators [Sam] Nunn [D-GA] and [William] Cohen [R-ME] realized it, and they legislated it.

If you read the history of how SOCOM was created, the Services did not want to give up their own individual special operations forces that had been created. Congress realized that it needed to strengthen joint interoperability, especially for high-risk missions. Needs were emerging as terrorism was popping up around the globe.

But what Congress did that specifically made SOCOM special was the unique acquisition authority that it directed—with specific funding that didn't have to go through the Services. That was really the power behind what created SOF.

Every time I talk to Congress, I talk about their key role in this—but then how much we value the oversight of Congress along with the civilian DOD side, specifically an ASD (SO/LIC) [Assistant Secretary of Defense for Special Operations and Low-Intensity

Conflict]. Congress directed its standup at the same time for that oversight aspect. That's an important part that aligns with the Constitution—with civilian oversight and a military accountable to civilian leadership. Congress asks me tough questions all the time, and they should. When we get congressional delegations into SOCOM headquarters—and to all our subordinates and overseas—we welcome those visits.

While we're a very small part—about 3 percent—of the DOD budget with about 2 percent of the force, Congress still pays an incredible amount of attention to us, and they should. The American public and Congress must trust in special operations forces, and we must sustain that every day.

*JFQ: Many conflict zones are not traditional ones and labeling these situations has become a popular industry with names such as gray zones, asymmetric warfare, and competitions short of war. How does your command describe these challenges and plan to account for them?*

**General Clarke:** None of us should be surprised by this. Our rivals have studied us, and they know that we have incredible and overwhelming power in our joint force. They won't challenge us directly. We expect them to seek advantage through asymmetric means. But that doesn't mean we shouldn't just keep moving along without paying attention.

SOCOM's position is that we can operate in this gray zone and counter our adversaries. We're born out of this. Go all the way back to our roots with the OSS [Office of Strategic Services] in World War II, when small teams jumped into France and helped the resistance forces.

That's one example of using asymmetric capabilities. Because at the end of the day, this is about undermining adversary confidence. They are going to think twice that their aggression can succeed or that it will be easy.

What SOF does is present multiple dilemmas. We expand those options to threaten what an adversary may hold

dear. We can place some of those adversary assets at risk. We can fight in the war around the edges without having to be directly involved. We set the conditions for that today.

Think about a place like the Baltics right now. We've been working with our Latvian, Lithuanian, and Estonian partners for decades in Afghanistan. But we're also with them right now in their countries training alongside them, looking at their resistance capabilities, and continuing to think about how they could, in fact, resist as nations.

I think this will be a great lesson as we look at potential conflict zones around the world—to be there before they start. Building those capabilities with our allies and partners presents an unmatched advantage. We have the culture and language capabilities and the understanding of what irregular warfare could be. For competition in the gray zone, it's not just our adversaries contending there, but SOF and the joint force can compete there as well.

*JFQ: Can you discuss how you see the impact of technology that used to be solely available to nation-states and their militaries but is now available to anyone who can buy it? What ways are you working to operate in such a world?*

**General Clarke:** There's multiple examples. Right now, one of the most pressing threats is the UAS [unmanned aerial systems] threat. These are the IEDs [improvised explosive devices] of the future. Everyone remembers 2003–2004 when the number one killer of our forces was IEDs—first in Iraq, and then it transitioned into Afghanistan. Now, an IED has wings and it can move. The wire that connected that IED or the remote device is now harder to defeat.

We're seeing our adversaries really pick up their game in this area—again starting in Iraq. You can clearly see where this technology of small UAS can grow. That's one example that is concerning.

We're also developing technologies and capabilities to counter them and then looking where we can be "left of launch" to

disrupt supply chains, transportation, [and] development before it's too late. Then we only have to defeat them "right of launch" when we're trying to shoot down the final UAS that could be coming at our forces.

The future of UAS leads to another technology—AI [artificial intelligence] and machine-learning. One example of using those and UAS together would be in swarming and remotely operated or independently operated technologies. We're really looking hard within SOCOM, training leaders in artificial intelligence and in machine-learning and exploring capabilities to counter those technologies.

The final technology I'll talk about is in the information domain. Our adversaries compete at very low cost, using misinformation and disinformation. We've got to develop technologies to counter those efforts by using AI and machine-learning to immediately identify and counter those messages before the narrative gets wide distribution. All of those are really important in today's environment.

*JFQ: U.S. Special Operations Command is also unique in that it is the only combatant command with an education mission that is embodied in the Joint Special Operations University [JSOU]. How will your command leverage this evolving professional military education capability to your advantage?*

**General Clarke:** Go back to our founding and that unique authority where we are required to oversee SOF-unique training. That's why we have a JSOU. That is tied to the broader joint education and training mission. That's still SOF truth number one: Humans are more important than hardware.

We must invest in those people by continuing to train and educate those innovative problem-solvers. JSOU sharpens the edge of SOF by investing in our junior leaders by training and developing them.

They're also specifically looking at the priorities of this command and where this command needs to go. They're developing coursework that is specific to those problems. And that unique training includes some of the

coordinating authorities—teaching specific classes on CWMD or teaching classes on the gray zone, campaigning, and integrated deterrence.

Because JSOU is on the SOCOM campus, it is deeply integrated with the staff. Our J5 and our JSOU president are closely linked for that thought process and for the development of the future SOF force. It's incredible what they're doing there. JSOU is involved in all our commanders' conferences to see where the command is going and how to be linked. I consider it one of SOCOM's most important resources in the training, equipping, and development of our force.

The other thing that JSOU does in addition to teaching is they do detailed research looking deep into some of our most vexing problems. As I talked about earlier with the J5, they're helping us solve those problems. That research is a big advantage for us, and some of it is cutting-edge. There's a huge ecosystem of civilian education programs and institutions that can really help us. They're going to places like NDU [National Defense University], but also going to Carnegie Mellon or the Fletcher School at Tufts to bring in expertise—whether on counterterrorism or WMD. JSOU really helps us in those areas, too.

*JFQ: How will the rise of the U.S. Space Force affect your command and special operations forces? As a force highly dependent on what the Space Force provides, what opportunities do you see for your command to assist in how the Space Force evolves?*

**General Clarke:** Space is a critical domain. SOF is and will remain reliant on space-based capabilities. But I also want space to view SOF as an enabler to space in the future.

I do think that a great triad can exist between cyber, space, and SOCOM. As I told Secretary [Mark] Esper as we were discussing operations in space, I said that I'd recommend we don't talk about *in* space, but we talk about this *for* space. The space capabilities start here on the terrestrial side. We have to protect our own capabilities, but we could also hold

adversaries' terrestrial base capabilities at risk.

SOF's unique access and placement can provide those opportunities in the future. We realized the importance of space and the need to continue to work very closely with SPACECOM [U.S. Space Command] and the Space Force to provide those capabilities for the joint, all-domain warfighting aspect.

*JFQ: As a graduate of the National War College who has obviously been successful in your post-joint professional military education experience, looking back on that year, what advantages did National Defense University provide you? What would you recommend to the faculty to consider when developing strategy related courses for future leaders like yourself?*

**General Clarke:** First, I thank NDU for that great year in 2006–2007. I had just finished about 5 years focused directly on combat. I had conversations about those experiences not only across the joint force but also with interagency partners and allies—to reflect on where we were going, where we'd been, and where we were going in the future. That exposure for me to all elements of our national command and infrastructure as well as our international partners was invaluable.

I had some world-class instructors who stretched me. But it was also a time to reflect and think. What I found was that year was just one step of what must be a lifelong investment in the profession and in continued study as a military professional. You cannot remain static. You must continue to read and develop. I have found that I read and study more in each subsequent year. The National War College gave me some ideas and gave me some frameworks to help look at problems into the future. JFQ



Army Green Berets assigned to 1<sup>st</sup> Battalion, 10<sup>th</sup> Special Forces Group, prepare to breach and enter building as part of Close Quarter Battle training in Germany, May 5, 2020 (U.S. Army/Thomas Mort)

# Rediscovering the Value of Special Operations

By Isaiah Wilson III

Today, America's special operations forces (SOF) face a moment of strategic inflection and identity reflection at the threshold crossing of two fundamental questions: How has the character of global geopolitical competition changed? What are the implications for the future roles, missions, and force structures (that is, future utility) of SOF for the 2020s through the 2050s? Even as the United States

enters this age, this new era brings new demands of striking a rebalance from its focus for the past two decades on countering terrorism, violent extremist organizations (VEOs), and insurgencies to coping with threats of confrontations between so-called Great Powers. Tomorrow's special operations and SOF must adjust accordingly.

## Lessons Gathered but Not Yet Learned?

Amid all the present-day ambiguities and grayness in all things, including security and defense matters, perhaps

the one thing crystal clear is that we must learn lessons from the past and make changes now to best face the future. And from such a "back to our futures" review, one lesson is clear: SOF is, as it has always been, a great value proposition for our country.

As we continue to think about and work through this question of (re)defining SOF's utility in Great Power competition (GPC), we need to go back to fundamentals. The win in this environment of competition is, as it has always been throughout the history of special operations, in "left-of-boom"

---

Dr. Isaiah (Ike) Wilson III is a Professor of Political Science and President of the Joint Special Operations University.

**Table. SOF Activities**

<p><b>MISO</b> Military information support operations are planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.</p>	<p><b>UW</b> Unconventional warfare consists of actions to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power.</p>	<p><b>CAO</b> Civil affairs operations enhance the relationship between military forces and civilian authorities in localities where military forces are present.</p>	<p><b>SR</b> Special reconnaissance consists of actions conducted in sensitive environments to collect or verify information of strategic or operational significance.</p>
<p><b>SFA</b> Security force assistance includes activities based on organizing, training, equipping, rebuilding, and advising various components of foreign security forces.</p>	<p><b>FID</b> Foreign internal defense is comprised of activities that support a host nation's internal defense and development strategy and programs designed to protect against subversion, lawlessness, insurgency, terrorism, and other threats to their internal security, stability, and legitimacy.</p>	<p><b>HRR</b> Hostage rescue and recovery consist of offensive measures taken to prevent, deter, preempt, and respond to terrorist threats and incidents, including recapture of U.S. facilities, installations, and sensitive material in overseas areas.</p>	<p><b>CT</b> Counterterrorism includes actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks.</p>
<p><b>C-WMD</b> Counterproliferation of weapons of mass destruction describes activities to support U.S. Government efforts to curtail the conceptualization, development, possession, proliferation, use, and effects of weapons of mass destruction, related expertise, materials, technologies, and means of delivery by state and nonstate actors.</p>	<p><b>CI</b> Counterinsurgency is the blend of civilian and military efforts designed to end insurgent violence and facilitate a return to peaceful political processes.</p>	<p><b>DA</b> Direct action includes short-duration strikes and other small-scale offensive actions employing specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets.</p>	<p><b>FHA</b> Foreign humanitarian assistance is the range of DOD humanitarian activities conducted outside the United States and its territories to relieve or reduce human suffering, disease, hunger, or privation.</p>

operations, activities, and investments. The key is comprehensive integrated deterrence. In other words, the win is achieved through placing the joint, interagency, intergovernmental, multinational force in positional advantage over competitors and adversaries through access, placement, and strategic influence, setting the conditions for the possibilities of winning before—or even without—the fight.

As the United States and the West learned in the 20<sup>th</sup> century, preventing the Cold War from going hot was an essential element in the theory of victory in the strategic rivalry between totalitarianism and communism on one side and democracy and capitalism on the other. The United States and its allies and partners achieved their geostrategic interests in the Cold War without fighting the Soviet Union directly in open armed conflict, and the same logic can apply in the 21<sup>st</sup> century.

GPC is the high end of a rising scale of international relations ranging from interactions of cooperation, competition, conflict, and classic war. The potential impact of SOF's utility in an environment of competition will demand, as it always has, anticipating, finding, and creating ways and opportunities that allow the Nation and its allies and partners to do two things simultaneously: lower the amplitude and the temperature of competition and conflict between competitors and deter and prevent a next Great Power war from happening at all.

SOF must compete in the information space and not concede to their adversaries. Today's new compound security normal for SOF will be to operate in remote, denied, and disrupted environments under ubiquitous intelligence surveillance with the threat of targeting by high-end military capabilities, including weapons of mass destruction, where the cyber and electronic warfare domains

are contested and increased scrutiny is routine. We will need to return to the ideas of special operations use and utility that empowers *SOF as Sentinel*, preparing the environment as the frontline ambassadors of the joint force and as the “first three feet” employed in any competition or confrontation zone.

**Rediscovering SOF for a New Age: A “Back to the Future” Approach**

To understand and appreciate SOF of the future, we must understand SOF then to now. From an organizational perspective, arguably, there have been three previous ages of U.S. special operations, beginning in World War II with the “Wild Bill” Donovan years and the Office of Strategic Services. The 1960s perhaps mark an official beginning of the second age of SOF. President John F. Kennedy was visionary in his efforts during this time to increase the capability



of the Department of Defense pointedly in the conduct of counterinsurgency and unconventional warfare, focused at the time, as President Kennedy stated plainly, “against the struggle against despotic insurgency.”<sup>1</sup> The so-called third age was the period of a global war on terror and finding China and Russia probing the perimeter of their spheres of prior influence and to an extent beyond. Key events marking the transition from this third age to the fourth age can be appreciated in compounding occurrences dating back to “spring movements” as early as 2006. These movements began with the orange and green movements of the Republic of Georgia, Ukraine, and Iran, continued through Arab variations of the same including Egypt (2010 and a second wave in 2013), Syria (2011), and the ongoing Syria-Iraq compound conflict (which began in 2014), just to name a few.

The U.S. and North Atlantic Treaty Organization (NATO) withdrawal from Afghanistan in late summer of 2021 may mark an ending of the third age. However, the fourth age is marked by a clear exploitation of traditional Western institutions and influence, especially at fragile geographic and sectoral nexuses and with the Russians and Chinese openly no longer playing by established rules and norms. One need look no further for examples than China’s island-building activities and Russia’s “little green men” territorial incursions.

### **SOF’s Enduring Value at the Intersectionality of Threats**

The new Interim National Security Strategic Guidance speaks to all these aspects and dynamics of a “compounded security threats” world in terms of an “intersectionality of threats.”<sup>2</sup> At the heart of such intersectionality lies a new security dilemma—the compound security dilemma—that today, much more than in the past, demands nothing less than a working at the nexuses and between the boundaries and seams of our own created divisions between matters of “defense and security” from the traditional and nontraditional “water’s edge” that separates the foreign from the domestic.

SOF have incredible value in this intersectional space. And they always have. SOF understand gray zones and are making sound adjustments to not only compete but also prevail. As we—in collaboration with the joint force, our interagency partners, and our foreign country allies—look ahead, SOF must once again gain the influence, leverage, and positional advantage (that is, physical, virtual/digital, and cognitive) necessary to compete and protect the Nation’s interests short of armed conflict while also establishing the ability to transition rapidly to combat if, when, and where required, enabling our country and its allies to deliver overmatching decisive combat power. Choosing the right tools at the right time and for the right problem to be solved is the most imperative gray matter requirement for SOF leaders today and for the SOF professionals of tomorrow.

SOF mission sets, in and of themselves, have not significantly changed. However, the environment in which they are conducted has continued to change significantly. This was true for the last 20 years that found special operators missioned more in roles of direct action, crisis response, counterterrorism, and counter-VEO profiles, but not exclusively so. One benefit of 20 years of countering VEOs is the strong ties we have to the interagency community, not to mention allies and partners. This was just as true throughout SOF’s prior 55 years of use and utility dating back to World War II. And this will remain true in future years.

SOF is tailor-made to conduct military information support operations, psychological operations, and influence operations. There will be great need for these capabilities now and in the future. Again, working with and through alliances and partnerships is not just a nice-to-have additive, but rather an essential part of any intended winning solution. Building partner capacity, advising and assisting indigenous resistance forces, and leveraging language and cultural knowledge are longstanding SOF strengths.

Operating with and by proxies and surrogates, through partners, and in the gray zone are just additional longstanding

SOF applied art and strengths. Using commercial-off-the-shelf equipment and being flexible, agile, and on the cutting edge of technology are other classic SOF strengths that will be as vital as we move into the fourth age.

### **Tech-Enabling Tomorrow’s SOF HE<sup>2</sup>RO**

The compound security character of the global security environment is such that it will demand a future utility of SOF that is equally compounded: a comprehensive combination of all the skills, techniques, and uses of technological and operational methods of all three preceding ages, amplified by 21<sup>st</sup>-century technological advancements. Nothing less than this comprehensive, joint-combined utility of SOF philosophy, culture, and approach is required for overmatching power in and under fourth-age conditions and in this period of rebalance for assuring an integrated deterrent power capacity for the Nation.

The dynamics of stability and control are changing as emerging technologies such as 5G, artificial intelligence (AI), and the Internet of Things lead to a decentralization of influence and less hierarchical political structures. Rapid advancement and proliferation of these new technologies is also redefining traditional views and norms on such things as what it means to win, what constitutes a crime, and what behavior is acceptable in (post) modern war. SOF leaders must be able to apply AI. Future SOF professionals must be (come) AI-ready leaders.

### **Special Operations as Part of Integrated Statecraft Solutions**

In addition, SOF’s utility must be considered not as transactional but rather transformational. The way we measure the return on investment on SOF must be measured in new ways that fully acculturate the interests and capabilities of allies and partners into our own national use and utility of force strategies and calculations. This is comprehensive joint-combined readiness.

Looking ahead, SOF force structure, capabilities, and design will also likely need to adapt significantly to this new

era. In this fourth age, geography has returned with a vengeance as a governing dynamic of international relations. Also, positional advantage is once again a determinative factor of this new compound security world (dis)order. This speaks to matters of geostrategy and is vital because attaining strategic influence from key geographical areas is an essential element to the disruptors' playbooks, and more pointedly, to China's expansion globally as they seek to couple targeted control and access to key geostrategic locations to outmaneuver and hold at risk U.S. interests regionally and globally.<sup>3</sup> And much of China's and Russia's actions are done in a manner that operates outside traditional boundaries set by long-standing international rules and norms.

While the United States cannot and should never envy such subversive approaches that seek to undermine the rules-based international order, much less attempt to replicate them, we can instead orient our efforts on positive aims that reinforce our democratic values and ideas that underpin our conceptions of political sovereignty and territorial integrity, the very cornerstones of the international system we seek to strengthen in our strategic competition with China and Russia as major power-brokering disruptor states along with other malign actors. We do this by helping our allies and partners in their efforts to build national resilience and resistance against predatory, subversive, gray zone threats and by helping to shape mutually beneficial security environments through our foreign assistance and security cooperation programs. As far back as its origins in World War II, support of national resistance and resilience operations has long been a core competency of special operations as well as a cornerstone to SOF's use and utility as an early indication and warning, strong-pointing, and "rheostat" capability for the Nation.

As we know, Russia, China, and Iran are deliberate in the what and the where of their activities, and it is the *where* that makes issues of geostrategy all the more relevant. For example, amplifying

around 2014, Russian operational reach in Crimea, Cyprus, Greece, Egypt, and Syria has been about ensuring that there is a buffer zone (Ukraine) between Russia and NATO, about holding the eastern Mediterranean sea lines of communication at risk, and about restoring Russia's role on the world stage.

When it comes to China's Chinese Communist Party (CCP), its economic activities through the Belt and Road Initiative (BRI) are significant indicators of China's global ambitions. China's efforts in Latin America involve gaining influence to place the Panama Canal in a series of overlapping influence levers to salami slice to a new normal of either control or positional denial of U.S. access, basing, and overflight, all while carving away support from Taiwan via BRI financial inducements to fragile democracies in the Western Hemisphere. With regard to Africa, China is outperforming the United States diplomatically and economically. China has more embassies in Africa than the United States, which erodes American influence and the dwindling support for Taiwan from previously friendly African states. China is now Africa's largest trading partner and the largest bilateral lender to many African countries, "creating an asymmetric power dynamic with the potential for dependency."<sup>4</sup>

Chinese strategists think and write using geopolitical terms, dividing the world up into regions or zones, and deploy concepts such as "heartland" and "rimland" in their works with frequent direct referrals to the great geostrategic theorists such as Sir Halford Mackinder and Alfred Thayer Mahan. SOF leaders need to think and act in geopolitical and geostrategic terms as well, particularly if they seek to achieve intellectual overmatch against their CCP and Kremlin counterparts.

We must also recognize that our competitors and adversaries have already redefined the notion of competition, even of warfare itself, and the role of their militaries within it. Loosely referred to as the *X* in special operations, objectives—or rather the specific goal that directs and purposes every military operation—have often been mistakenly considered only in terms of the physical

domain.<sup>5</sup> The concept of the *X* has now become all-domain, demanding a reframing of the way we fight in the future and a reframing of even what constitutes a fight itself. In the fourth age and under conditions of compound security, special operations professionals must be trans-domain problem-solvers. A geostrategic positional advantage approach also forces a competitor or adversary to focus their resources at what the famed George Kennan called the "strong points."<sup>6</sup>

For this next age, we will need SOF to play point-versus-area defense at or proximate to these geographic, human security, and cognitive strong points. And in so doing, it is important to note that the point of action may be far removed from the point of effect. And in that sense, SOF can indirectly affect behavioral and decisionmaking calculations through actions that may be in other physical and nonphysical (for example, virtual, cognitive, and ideational) domains. This is the exact logic of placing combined joint interagency task forces (CJIATFs) within combined joint special operations task forces placed at or proximate to the geostrategic nexuses.

SOF has employed this logic worldwide and through several evolutions of the find, fix, finish, exploit, analyze, and disseminate actionable-intelligence CJIATF process. For example, in Iraq, SOF Task Force 714 was able to adapt to the mission of finding and dismantling al Qaeda in Iraq through the fusion of interagency, intergovernmental, and allied and foreign country partner collaboration, producing the very sort of big data-supported, intelligence-driven operations throughout and at key critical locations across a vast theater of operations and activities that is intended when we speak of whole-of-government solutions.<sup>7</sup> It is through such command and control and force-projection platforms—strategically placed, sustainable counterterrorism plus GPC platforms—where use (employment) and utility (service provision) of SOF can and must be combined and integrated and where and how compound threats can be overmatched in cost-effective ways.

Special Forces Soldier assigned to 10<sup>th</sup> Special Forces Group demonstrates chemical light "buzzsaw" used to signal incoming aircraft at night, May 10, 2021, in North Macedonia, during exercise Trojan Footprint 21 (U.S. Navy/Rob Kunzig)





Two Navy Special Warfare Combatant-Craft Crewmen assigned to Naval Special Warfare engage target during joint live-fire training exercise with Hellenic navy operators from Underwater Demolition Command, in Aegean Sea near Greece, July 16, 2020 (U.S. Army/Aven Santiago)

### Another Case in Point: Syria

We need to look no further than SOF's operational placement in and throughout northeast Syria since 2014 and how that presence and those roles have evolved over time for proof of principle of SOF's utility beyond counterterrorism and counter-VEOs, beyond the context of the war on terror, and moreover, as an expression of integrated deterrence in action. What began as an effort to destroy the physical manifestations of the caliphate through direct action, raids, and strikes, many times in concert with state and nonstate actors committed to defeating the so-called Islamic State (IS), quickly became a mission to deter further Russian (and Turkish) territorial provocation, assure new partners (Syrian Kurds), deny freedom of action to Iran and its surrogates and proxies, defend critical resources and infrastructure, deny any resurgence of IS as an existential threat to friendly regional governments, and maintain U.S. access and influence where the East and West truly converge.

The fact that the U.S. Government did this with such minimal investment, while assuming acceptable risk, must be understood and appreciated, even lauded, for what it was: a new paradigm in which the use and utility of SOF goes well beyond its two decades of direct action merely in the *context* of counterterrorism, but instead where direct action and counterterrorism are integral use-of-force activities endemic to, and not separate or separable from, GPC.

In this enlarged context, from use to utility of force, SOF serves as the regulating rheostat for a new geopolitical environment that challenges conventional wisdom but demands new ways of thinking and acting toward an array of threats, state and nonstate, and the underlying conditions that drive them.

### Implementing Change: The Future of SOF Professionals

*We will maintain the proficiency of special operations forces to focus on crisis response and priority counterterrorism and unconventional warfare missions.*

*And we will develop capabilities to better compete and deter gray zone actions.*

—Interim National Security Strategic Guidance

In today's strategic environment, information technology has significantly enabled action in the cognitive domain. For SOF, the cognitive domain is the primary medium through which we operate. As we transition through an era of attempted strategic control, we will move into an era of strategic influence, the currency of (Great Power) competition. This demands a new SOF H.E<sup>2</sup>.R.O.<sup>TM</sup>—the highly educated, hyper (tech)-enabled, responsible operator. This comprehensive SOF utility for the future will produce:

- continuous integration of national instruments of power and influence in support of national objectives
- an unprecedented degree of global integration of the all-domain resources available from the combatant commands, Service component commands, and theater special operations commands to generate

- advantage for ourselves and dilemmas for our competitors
- assured access through strategic shaping and support to resistance and resilience strong-pointing of allies and partners
  - critical and creative strategic thinking across the Joint Staff and other joint headquarters and approaches to joint warfighting
  - highly effective coalition, allied, international partner, and U.S. coordination and integration
  - deeper understanding of the implications of disruptive and future technologies for adversaries and ourselves.<sup>8</sup>

At U.S. Special Operations Command (USSOCOM), our Campaign Plan for Global Special Operations is our blueprint. We are focusing in real investment terms on making informational advantage and influence operations, adding both as new tips-of-spears to SOF's quiver of capabilities. USSOCOM's recently created Joint Military Information Support Operations WebOps Center is only one example of the types of new emphases on new operations, activities, and investments reflecting a rediscovery of the full utility of special operations.

The future focus of special operations will be what it has always been: to remain exquisite, proactive, and aimed at solving problems in ways that avoid moral injury to the Nation. This imperative has always found the country's special operators, working with and through allies and partner forces, in the gray zones between competition, conflict, and war. As it has always been, so it shall continue to be. JFQ

## Notes

<sup>1</sup> United States Special Operations Command, "Guidance on Briefing Notes," available at <<https://slideplayer.com/slide/9402754/>>.

<sup>2</sup> White House, *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), available at <<https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>>.

<sup>3</sup> *Geostrategy* is a subfield of geopolitics, a type of foreign policy guided principally by

geographical factors as they inform, constrain, or affect political and military planning. It is the systematic analysis to develop a sensitive understanding of geographical realities, political forces, historical experience, and the factors that change these to formulate prescriptions on the application of military power to achieve vital objectives. Derived from the Center for Strategic and International Studies' Brzezinski Institute on Geostrategy, available at <<https://www.csis.org/programs/brzezinski-institute-geostrategy>>.

<sup>4</sup> Landry Signé, "How to Restore U.S. Credibility in Africa," *Foreign Policy*, January 15, 2021, available at <<https://foreignpolicy.com/2021/01/15/united-states-africa-biden-administration-relations-china/>>.

<sup>5</sup> U.S. Special Operations Command, "SOF 2030," February 7, 2020, 14.

<sup>6</sup> Giles D. Harlow and George C. Maerz, eds., *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946–47* (Washington, DC: NDU Press, 1991), available at <[https://www.files.ethz.ch/isn/139669/1991-05\\_Measures\\_Short\\_War.pdf](https://www.files.ethz.ch/isn/139669/1991-05_Measures_Short_War.pdf)>.

<sup>7</sup> Richard H. Schultz and Richard D. Clarke, "Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare," *Modern War Institute* at West Point, August 25, 2020, available at <<https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/>>.

<sup>8</sup> *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education & Talent Management* (Washington, DC: The Joint Staff, May 1, 2020), available at <[https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs\\_pme\\_tm\\_vision.pdf?ver=2020-05-15-102429-817](https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817)>.

## New from NDU Press

for the Center for Strategic Research

Strategic Forum 308

*Baltics Left of Bang: The Southern Shore*

By Marcel Hadeed, Mariusz Kaminski, Monika Sus, Brett Swaney, and Amelie Theussen



Detering and defending against Russian aggression in the Baltic Sea region prior to open hostilities,

or "left of bang," is a political problem that requires a coordinated regional approach by the Baltic southern shore states—Poland, Germany, and Denmark—in conjunction with their North Atlantic Treaty Organization (NATO) and European Union (EU) allies. Despite common membership in NATO and the EU, the southern shore states hold differing strategic perspectives that reflect the challenges of a coordinated approach. These states should prioritize Baltic maritime security, regional mobility, and unconventional warfare capabilities in coordination with regional allies and partners. They should also leverage or enhance EU capabilities in cyber, information, and strategic communications to better deter and defend against Russian hostile measures.



Visit the NDU Press Web site for more information on publications at [ndupress.ndu.edu](http://ndupress.ndu.edu)



Air Force special tactics operators assigned to 24<sup>th</sup> Special Operations Wing conduct hoist operations with Navy MH-60 Seahawk aircrew members assigned to Helicopter Sea Combat Squadron Nine, during Emerald Warrior 21.1, at Hurlburt Field, Florida, February 18, 2021 (U.S. Air Force/Edward Coddington)

# Making the Case for a Joint Special Operations Profession

By Isaiah Wilson III and C. Anthony Pfaff

The year 2021 proved a period of strategic inflection, a moment of standout changes in the character of geopolitical competition. Arguably, the last similar period of such strategic inflection began with the terrorist

---

Dr. Isaiah (Ike) Wilson III is a Professor of Political Science and President of the Joint Special Operations University. Dr. C. Anthony Pfaff is a Research Professor for Strategy, the Military Profession, and Ethics in the Strategic Studies Institute at the U.S. Army War College and a Senior Nonresident Fellow at the Atlantic Council.

attacks of 9/11, what scholars and practitioners comfortably regard as a historic watershed event in international relations. Those attacks gave rise to what became known as the war on terror. Just as there was a great deal of uncertainty in 2001 of how best to prosecute a war on terror, there is now a great deal of uncertainty regarding how best to compete against peer and near-peer competitors who pose challenges in the current inflection. How to strike an effective strategic rebalance

between those functional imperatives that have defined the war on terror and the imperatives of the coming era only further complicate the situation.

Moreover, the experience of two decades of counterterrorism (CT) and counterinsurgency (COIN) operations in Afghanistan and Iraq suggests that this uncertainty may be unresolvable. While both wars have nominally ended, the doctrinal debates they inspired rage on. These conflicts have now largely defined the context and character of

special operations forces (SOF) and perhaps too narrowly focused them on the three counterforce operations, activities, and investments of CT, counter-violent extremist organizations, and COIN. However, while special operations and SOF played a vanguard role in rediscovering and refining tactics, techniques, tradecraft, and incorporating new technology for waging the fights during the war on terror, their successful operations alone did not always translate into lasting strategic success.

As SOF transition operations to support competition with peer and near-peer competitors, there is persistent frustration over apparent U.S. failures. At the time of this writing, China continues to provoke its neighbors in its near abroad while expanding its influence in Africa and South America. Russia, prior and in addition to the invasion of Ukraine, has successfully prevented its neighbors from strengthening ties with the West as well as challenged the United States in Syria. Iran, for its part, has limited U.S. influence in Iraq, Yemen, and the Levant through its use of proxies and terror operations. In each of these cases, it can seem that there is little the United States—especially the U.S. military—can do to reverse these developments.

This frustration, of course, is not the fault of SOF. International competition is best accomplished through the coordinated efforts of a variety of Services and agencies. SOF, however, are in a unique position to participate. However, as described in the 2020 U.S. Special Operations Command (USSOCOM) *Comprehensive Review*, a high operating tempo (OPTEMPO), coupled with statutory and resource limitations regarding SOF assessment, recruiting, and professional education, currently limit SOF ability to expand their role.<sup>1</sup> To do so, SOF will have to establish the kind of institutional infrastructure that can transform them from highly skilled operators to a joint special operations forces (JSOF) profession where certified professionals exercise autonomy over a specific jurisdiction. Mature professions provide a public good over a jurisdiction, as in health care where certified professionals such

as doctors and nurses exercise autonomy regarding how to best to serve their clients. Providing that public good requires more than just skill at task execution; it requires robust institutions capable of building and maintaining client trust by certifying persons in those skills as well as governing how those skills are employed and holding professionals accountable for the service they provide. Currently, due largely to statutory limitations, SOF have no unique jurisdiction; they are limited in their ability to certify and govern the employment of SOF operators.

This article seeks to introduce for consideration and debate this question of whether there is now a need for a formal JSOF profession. University of Chicago sociologist Andrew Abbott argues that the purpose of a profession is to diagnose, infer, and treat problems that arise within its jurisdiction. How, when, and where a profession accomplishes those functions largely establish practitioners' identity, which is expressed as shared standards, norms, and laws that collectively place the professional in a better position to serve a social good than the nonprofessional. That positioning is what gives the non-professional client reasons to trust not the professional but the profession itself. That trust is then expressed in terms of the autonomy that society grants professionals to exercise their expert knowledge. In this context, the opportunity for SOF is clear: claiming a jurisdiction within the context of international competition will place SOF in a better position to build trust and assure autonomy. Doing so will require clarity on what counts as expert knowledge (as opposed to skills and tasks) and the necessary institutional development to certify SOF professionals in the application of this knowledge.

### **Rethinking Joint-Combined SOF from a Systems of Professions Point of View**

Abbott's framework, drawn largely from his seminal work in sociology, has new relevance to the Armed Forces' professions in the 21<sup>st</sup> century, and we propose even more relevant application to the questions regarding the professional status of special operations

and SOF use and utility, particularly in the context of joint and combined integration.<sup>2</sup> By *integration*, we refer to the imperative of approaching complex, complicated, wicked, and compounded challenges through “whole of governments, whole of societies,” multilateral ways, means, and coordinated ends. The lack of jointness (that is, cross-Armed Forces' SOF component's interoperability) was a major finding of the Holloway Commission Report in the wake of the tragic Iranian hostage rescue mission, Operation *Eagle Claw*, more popularly referred to as *Desert One*.<sup>3</sup> Today, under compound security conditions, similar operational needs-based arguments for greater integration (extended now well beyond joint) to full joint, interagency, intergovernmental, multinational, and commercial (JIIMC) dominate, defining the central logic of the 2022 U.S. national security, defense, and military strategies. Joint integration in the past and JIIMC integration now and into the future find SOF once again of central focus—JIIMC integration is the new functional imperative.

Abbott's model portrays professions locked in competition for jurisdiction over once solvable problems that have become relatively and suddenly more intractable.<sup>4</sup> For example, in the bipolar, relatively unnetworked geostrategic environment of the 20<sup>th</sup> century, nuclear overmatch coupled with technologically advanced conventional forces seemed sufficient to deter/contain peer adversaries. In today's globalized, multipolar environment, weaker adversaries can exploit technology to bypass military strength to place the United States at strategic disadvantage and undermine U.S. interests.

In this context, Abbott's distinctive contribution to the discourse is to methodically define professions “wholly in terms of an elbows-out application of expertise; professions compete with each other for expertise-based jurisdiction over solvable problems.”<sup>5</sup> According to Abbott's systems of professions theory, competition can arise when social or technical changes act to weaken an existing profession's jurisdiction or to create an entirely new niche, as with the proliferation



Air Force MC-130H Combat Talon II aircraft loadmaster assigned to U.S. Special Operations Command Central observes Marine Corps MV-22 Osprey aircraft assigned to Marine Medium Tiltrotor Squadron 164 Reinforced, 15<sup>th</sup> Marine Expeditionary Unit, as it receives fuel during tiltrotor air-to-air refueling over undisclosed location, March 10, 2021 (U.S. Air Force/Trevor T. McBride)





of computers.<sup>6</sup> The outcomes of competition may be that one profession seizes turf from another, or there may be one of several forms of negotiated symbiosis.

Central to Abbott's model is his definition of *profession* itself, wholly founded on this competitive process. To Abbott, an occupation is a profession if (and only if) it can abstract its knowledge not only to solve novel problems but also to adapt its practices to new niches.<sup>7</sup> Abbott argues, "Many occupations fight for turf, but only professions expand

their cognitive domain by using abstract knowledge to annex new areas, to define them as their own proper work."<sup>8</sup> An equally valuable contribution of Abbott's work to the questions central to this article is Abbott's invocation of a classic healthcare metaphor of *diagnosis* → *inference* → *treatment* as a model of all professional problem-solving.<sup>9</sup> In this article, we apply this model (but present it nonlinearly) as a device to diagnose the potential needs of a JSOF profession and to infer a potential treatment therein.

### **Diagnosis: Fragmented Professional Development Complicated by a Dramatically Altered State of Global Security and Stability**

*Diagnosis*, in this sense, metaphorically involves framing a problem in terms of the profession's known and reconsidered domain of expertise. Applied to the questions of this initial study, the inability to locate special operations clearly and definitively and SOF in a prior, clearly delineated jurisdiction



Navy SEALs conduct military freefall jump from C-2 Greyhound from Rawhides of Fleet Logistics Support Squadron 40 during training above Chesapeake Bay, Virginia Beach, July 7, 2020 (U.S. Navy/Scott Fenaroli)

may be an artifact and signal of a profession under the stressors of change in mission, orientation, applicability, or even identity, or the absence of a formal profession altogether.

As the USSOCOM *Comprehensive Review* candidly and publicly acknowledged, high OPTEMPO has resulted in a bias toward employment, often without a clear understanding for how such employment relates to achieving strategic ends.<sup>10</sup> The result has been a stressed force focused on the immediate task but not the long-term objective. Another major contributing factor to the 20-year tendency toward fragmented SOF professional development has been the statutorily directed dependency of SOF on the conventional forces for most recruitment, assessment, certification, and professional development. These two factors are related. Given the high demand for employment and the limited relevancy of conventional professional military education, there is little incentive to take advantage of professional development opportunities that do exist and the limited means to create ones unique to special operations.

Other critical factors and areas of relative gapped leader focus, capabilities, and capacities resourcing revealed in the USSOCOM *Comprehensive Review* include a recognized emphasis on physical and tactical skill training at the expense of focus on broader education and professional development, arguably contributing to a general sense of entitlement growing with and within a limited joint governing ethic.<sup>11</sup> When combined with the dramatic changes in the character of global competition, it is not hard to see why applications of force prove more and more anemic—proving too little, applied too late to prevent, and applied not long enough and in the right ways to solve problems in sustainable ways.

### **Treatment: Joint Professionalization and a Joint-Combined SOF Profession**

Abbott's metaphor of *treatment* draws from the available toolkit of a given profession. For special operations and SOF, this toolkit typically relates to 12

classic SOF core activities (also referred to as core tasks):

- military information support operations
- unconventional warfare
- civil affairs operations
- special reconnaissance
- security force assistance
- foreign internal defense
- hostage rescue and recovery
- counterterrorism
- counter-proliferation of weapons of mass destruction
- counterinsurgency
- direct action
- foreign humanitarian assistance.

Of course, these 12 activities do not comprehensively describe the abstract expert knowledge necessary to operate in hybrid contexts; however, they do represent a good start, the completion of which is one task SOF must fulfill to fully professionalize.

Moments of geostrategic change, transformation, transition, and threshold crossings herald new unknowns that challenge previously “known knowns.” Confidences in and questions over established jurisdiction regarding both diagnosis and treatment are susceptible to these changes; history shows these competitive challenges often, if not mostly, come in the form of new technologies or expertise claims from competing professions, often driven by dramatic changes in the demand-to-supply dynamics defining of that occupation's and/or organization's prior understandings of its value proposition and public service relevancy.

Today's rebalance toward a presumably new era of strategic competition, integrated deterrence, and active campaigning (cornerstone concepts underpinning the 2022 national defense and military strategies) is already giving an amplified and accelerative rise in competitions between and within the public service professions characterizing the national, global security, and defense establishment(s)—competitions of a character of change that inevitably incite fundamental reconsiderations of previous knowns regarding uses and utilities of

force and core versus peripheral identities (that is, the functional imperatives of the individual professional as well as the collective profession itself).

At times and under conditions of transformational disruptive change, foundations of the profession are questioned, at times even shaken, at their core four tenets: jurisdiction(s), expertise and expert knowledge, and culture (ethic and ethos), culminating in (re)defined functional imperative(s). The following are general (and generalizable across varied professions) term descriptions of these four tenets:

- **Jurisdiction:** A domain where diverse skills can integrate to achieve a social good, such as health, justice, or security.
- **Expert knowledge:** Technical, political, human development, and ethical knowledge that is abstract, legitimizes professional work, and establishes how the profession conducts research on, diagnoses, treats, and makes inferences regarding the problems its professionals are supposed to solve.
- **Autonomy:** The principle that professionals have authority (are licensed by the client, that is, society) to apply this expert knowledge over the jurisdiction and nonprofessionals do not.
- **Certification:** Institutional certification of not only skills but also professional knowledge at every level for which there is a problem the profession is supposed to solve.
- **Professional ethic:** Governing the profession to maintain trust of the client, which is informed by the profession's functional imperative, moral norms reflecting client values, and law.<sup>12</sup>

Professionalizing provides an *infrastructure* for rebalancing bureaucratic requirements with a professional ideal, for integrating other efforts to address psychological and physical conditions for ethical failure, and for attaining not only the knowledge but also the authority granted to professions versus their intended supporting bureaucracies (see table).<sup>13</sup>

Understanding the distinction between the characteristics of a profession

**Table. Profession vs. Bureaucracy**

Profession	Bureaucracy
Expert knowledge	Non-expert knowledge
Accepts lifelong learning	"You develop me"
New situations	Routine situations
"Practice" by humans	Work done by all
Unlimited personal liability	Little personal liability
Invests in humans first	Invests in SOPs, hardware
Measure = effectiveness	Measure = efficiency
Trust relationship with client	Public transactional relations
Granted some authority	Closely supervised
Develops worldview	No imposed viewpoint
Maintains ethos, self-policed	Externally imposed rules
Intrinsic motivations	Extrinsic motivations
A lifelong calling	A "job"

*Source:* Don M. Snider, "The Army Profession and Ethic," symposium presentation, Command and General Staff College Ethics Symposium, Center for the Army Profession and Ethic, December 4, 2012.

and those of a bureaucracy is important. There are times when the military should act as a bureaucracy—when it performs routine things, such as the annual budget process. Just as the medical profession should guard against arguing for doctors' parochial interests (instead of the interests of patients and overall health care) in the national healthcare debate, military officers must guard against wrongly using their specialized expertise merely to advance a bureaucratic agenda. Doing so could sacrifice the value of professional advice and relegate the military to being considered as just another interest group.<sup>14</sup>

As the United States grapples with the post-9/11 conditions of new enemies, new battlespaces, and new kinds of wars, military officers and perhaps especially the commissioned, noncommissioned, and warrant officers of the SOF community should avoid at least three traditional pitfalls typically associated with times of geostrategic ambiguity, budget stringency, and force reductions:

- becoming overcommitted to the latest technological trends at the expense of historical military challenges
- being tempted to rename, oversell, and fetishize new war concepts, especially in support of single-Service parochial interests

- overlaying the "hollow force" card, asserting that any reduction will irreparably degrade national security.

Instead, military effectiveness needs to be seen, understood, appreciated, and approached from a comprehensive, multi-Service perspective. Military professionals need to focus on maximizing national security while recognizing the fiscal impact that military spending has on overall national power.<sup>15</sup> This is uniquely and peculiarly true for SOF professionals and a joint-combined special operations forces (J-CSOF) profession.

### **Inference: Professionalize J-CSOF**

However, it is *inference*—the uncertain space between diagnosis and treatment that defines professional expertise—that also represents a great deal of vulnerability.<sup>16</sup> When the needed inference is simple (that is, a narrow "say-do gap" to be traversed, mitigated, or outright eliminated), the new required work can be automated or claimed by subordinate occupational groups, such as clerks and technicians, with no demand for whole-cloth change of the occupation. An example of this simple inference would be the automation of critical and physically demanding tasks or functions permitting the change or elimination

of certain biophysical requirements as exclusionary in accession and selection talent management processes. Yet when the inference is complex, the result may herald the birth of a new profession and/or the death of others.

SOF undergo rigorous selection and training that sets them apart by a unique functional imperative and body of expertise and expert professional knowledge from their parent Service, creating a greater bond among special operators who often identify first as being part of special operations and second as having originally joined their specific Service. Those areas of expert professional knowledge include:

- achieving information advantage and strategic influence
- leveraging emergent technologies to develop strategic-operational intelligence
- promoting ethical leadership in ungoverned spaces
- supporting national resilience and resistance to authoritarian disruptors
- advancing national interests in compound security competition.<sup>17</sup>

Related to the last area of expert professional knowledge, the Syria problem is a perfect but tragic example. Syria was and remains not one single conflict but rather a four-in-one compound war. It is part insurgency against the Bashar al-Asad regime, part counter-Islamic State coalitional war, part Syrian civil war in the making, and a war of forced extra-territorial human migration. Despite the United States demonstrating a high degree of skill at working with indigenous forces, Syria remains a low-rent quagmire for the United States with no end in sight. Thus, the inference is figuring out where the responsibility lies for resolving the quagmire in the favor of the United States, which then indicates who should determine how best to solve not only *that* problem but also *other* problems of a similar character.

As noted, SOF are uniquely suited to operating in such complex, hybrid environments. But because SOF do not conceive of this environment as their unique jurisdiction, they have so far not

developed the expert knowledge necessary to fully realize U.S. interests in this space. Moreover, they lack the institutional depth to manage how this expert knowledge affects their functional imperative.

### Unique Expertise and Expert Knowledge

Being and becoming more anticipatory is the new imperative leader attribute to attain the intellectual overmatch desired by the Chairman of the Joint Chiefs of Staff<sup>8</sup> to confront compound security threats that define the evolving character of global geopolitical competition.<sup>19</sup> Equally imperative is building a “strategic mindedness” within the current and

future SOF leader-operator—equal and matching to that same operator’s operational acumen—and finding and making new ways and moments of building this in earlier, more consistently, and continually throughout the full life cycle of JSOF professional officership development, cradle to *SOF for Life*.<sup>20</sup>

Expertise in the core competencies of hybrid warfare against state and nonstate adversaries, integration of information operations, cyber operations, foreign direct assistance, limited kinetic operations to achieve political objectives (that is, political warfare), and discrete, covert, and clandestine adversary denial operations, activities, and investments all

define the core of JSOF unique expertise and knowledge, along with SOF’s classic roles as escalation ladder “rheostat” and “sentinel” (that is, indication and warnings sensor-shooter capability), all while avoiding escalation to war.

It is important to recall that a key determinant (the distinction) between a general functionary and that of a unique profession lies in the matter of certification. For certification of JSOF as a joint profession, the SOF enterprise as an institution certifies not just or only along the lines of skills, activities, or tasks but also professional knowledge (core competencies) at every level for which there is a problem the profession is supposed to solve.



Army Green Beret assigned to 1<sup>st</sup> Battalion, 10<sup>th</sup> Special Forces Group, fires pistol during Army Marksmanship Unit sanctioned pistol competition, July 7, 2021 (U.S. Army/Thomas Mort)



Air Force special tactics officer communicates with AC-130J gunship during live-fire demonstration held for senior leaders of North Macedonian army and members of U.S. Embassy, May 11, 2021, during Trojan Footprint 21 (U.S. Navy/Rob Kunzig)

After 18 months of a rigorous and still running comprehensive, J-CSOF education, leader preparation, and development curriculum and training programs of instruction review and refit study, the Joint Special Operations University has identified—(re)discovered—five JSOF core competency knowledge arenas presently missing from (gapped) current Service SOF doctrine:

- Uses and utilities of JSOF in compound security competition (i.e., SOF in support of 21<sup>st</sup>- century irregular warfare)
  - SOF support to resilience and resistance operations
  - SOF support to economic statecraft
  - SOF support to strategic-operational shaping (“unconventional” deterrence)

- Informational advantage and strategic influence
- SOF as profession (SOF leadership and the SOF professional ethic)
- SOF and strategic-operational intelligence and emergent technology
- Design-based integrative campaigning and support to statecraft

SOF mission sets, in and of themselves, have not significantly changed. However, the environment in which they are conducted has continued to change significantly. Yet amid all this change, tomorrow’s fourth-age SOF leader-operator will always need to be comprehensively versed in the following core arenas—derivative from, as well as generating of—these five JSOF common core competencies: geostrategy and transnational affairs, strategic intelligence and integrative JIIMC operations, science and

technology and futures, and SOF leadership and the SOF professional ethic.

### **A Unique J-CSOF Functional Imperative**

The compound security character of the global security environment is such that it demands a utility of SOF that is equally compounded (that is, a comprehensive combination of all the skills, techniques and technics, and operational methods of all three preceding ages of SOF, amplified by 21<sup>st</sup>-century technological advancements). This, in short, speaks to the imperative of revisiting competition and rediscovering SOF historic roles, missions, and identity.

This does not mean SOF will not have a warfighting function. Neither does it mean other Services will not play a role in competition. What it does

mean, in Abbott's terms, is that SOF will "elbow" their way into owning something no other Service currently fully embraces. Consequently, and from a professional viewpoint, SOF must grapple with and find answers to core questions that define the coming strategic competition era, such as:

- What are the new modes of competition already seen today as well as ones that adversaries are likely to initiate?
- How can the U.S. shift from merely reacting to these and instead become more opportunistic?
- What are the limits of what SOF can do and what help must they seek from others?

The key—the ultimate functional imperative—then, of a J-CSOF profession is to apply SOF for the Nation's power purposes in ways and at points along the continuum of competition that defend and deter against the adversaries' "disruptor's playbooks" (that is, asymmetrical and irregular competitive and warfare techniques) within the gray zone (below thresholds of armed conflict) through credible presence and preparedness of compellent force.

Relating to the autonomy granted to a JSOF profession, SOF and USSOCOM will be (come) lead organizations for hybrid operations, leading in the integration of Service/JIIMC capabilities to deter and compel adversaries below the threshold of war. Professional certification brings an imperative of aligning Service programs' training tactical skills with SOF professional needs and pointedly from the joint, allied, partnered SOF perspectives, establishing higher level training and education to certify professionals at operational and strategic levels. All this in combination will demand a professional ethic that establishes a JSOF professional ethic governing competition and hybrid operations with special focus below the contact layer of the threshold of conflict. As a joint-combined profession, we argue that SOF will need to play a leading role in these additional three critical areas.

*Understanding and Redefining the Future Value of Alliances.* All the

still-under-draft (at the time of this publication) 2022 U.S. national strategic documents—security, defense, and military—emphasize the importance of allies and partners to affect integrated deterrence through active campaigning. There can be no say-do gaps in this functional imperative; such gaps will manifest holes-in-government nonsolutions—the stuff of self-inflicted "Thucydides traps." If the U.S. continues to diminish its support for and its valuation of alliances, what would SOF look like without such alliances?

*Redefining Information Operations.* After decades of being out-hustled and out-messaged by far more agile adversaries and their disinformation campaigns, the United States needs to level, rethink, and then rebuild its approach and methods to messaging so that it can fight and win the battle of the narrative. SOF, in JIIMC configurations, must return to their classic global scouting and sentinel roles and functions and accept a leadership role in redefining SOF roles in strategic-operational influence and information advantage operations, activities, and investments.

*Technological Development.* Developments today in robotics, artificial intelligence, quantum computing, and a wide variety of other areas may lead to astounding new capabilities that radically change human life and how humans interact with technology. As technological innovation and proliferation continue to accelerate rapidly, how can SOF adapt themselves to better leverage technology for their own use and better prepare for its use by adversaries?

Bedrock to the functional imperatives of a JSOF profession will be SOF's roles in the overdue revisitation of deterrence and SOF's classic roles therein. Since the ending of the Cold War, there has been a precipitous decline in practical experience with and knowledge of the theories, history, and practice of deterrence (simply defined as the action of discouraging an action or event through instilling doubt or fear of the consequences). If the change in the character of geopolitical competition does in fact find, among many factors and variables, a return to a

new 21<sup>st</sup>-century form of Great Power competition, then the recovery of our understandings of deterrence (and its relationship with compellence theory and praxis) and its differing types (including recognizing several important complexities of deterrence such as distinctions between specific and general deterrence, absolute and restrictive deterrence, and actual and perceived punishments<sup>21</sup>) is of vital importance.

How does the utility of SOF need to be relearned, reconceived, and recalibrated as a more effective instrument of strategic-operational escalation/deescalation management? This issue and the questions it raises is perhaps the most important (re)defining factor of SOF utility, purpose, and relevancy. It is perhaps the fundamental gray matter puzzle to be solved as J-CSOF campaign in the gray zones.

## Conclusion: Epilogue as Prologue

Any move toward a J-CSOF profession will be a heavy lift, to say the least. (Re)defining JSOF profession jurisdiction will have necessary, imperative overlaps with the Services, requiring some consensus and cooperation; however, the autonomy that comes with being its own profession will permit greater focus on unique-to-SOF professional development requirements. Eventually, SOF will require deliberate guidance on whether and how to continue functioning as a "quasi-Service." Specifically, decisions will be required to address each of the following concerns:

- SOF-related skills are not additive.
- Integration at higher levels is critical.
- New professional military education infrastructures are likely required (especially for senior officers and noncommissioned officers).
- Paucity of law and ethics below the threshold of armed conflict requires research and advocacy.

It is appropriate to conclude by speaking to the importance of the professional officer commissioning oath. Returning to S.L.A. Marshall's classic work, *The Armed Forces Officer*, both Marshall and George C. Marshall, Secretary of Defense at the

time, emphasized the linkage of the officer corps with service to Nation: “Thereafter, [the officer] is given a paper which says that because the President as representative of the people of this country reposes ‘special trust and confidence’ in his [or her] ‘patriotism, valor, fidelity, and abilities,’ he [or she] is forthwith commissioned.”<sup>22</sup>

S.L.A. Marshall went on to highlight one quality in particular: fidelity. *Fidelity* is commonly considered faithfulness to something to which one is bound by pledge or duty. In spite of all the formal rules and legal statutes obligating the commissioned and noncommissioned officer to the Constitution, and through it, to the American people, officer fidelity has proved to be the most enduring tie that binds officership and the profession of arms to the Nation. This bond has helped the Nation weather many storms, both foreign and domestic. The fidelity of the military professional has always found its strongest roots in the rich soils of American history. Examples set by leaders from General George Washington to Admiral William McRaven reinforce the principle of subordination of the military practitioner to civilian authority, and through that authority, to the defense of the Nation.

Special operations personnel address unique, specialized, and difficult military problems that require exceptionally trained, superbly equipped, and tremendously supported warfighters. While other Services can overwhelm enemies with massive combat power, special operations provide discreet, sometimes covert, precision military capabilities that have become increasingly relevant in modern warfare but have at the same time, over the past 20 years, come with its own gray area legal and ethical ambiguities and complications. The compound security dilemmas of today and tomorrow demand a restriking of that critical balance between SOF’s specialized warfighting and the Nation’s core values in a fourth-age, JSOF professional ethic. JFQ

*The authors acknowledge Lieutenant Colonel Joseph Long, USA (Ret.), Special Forces, Ph.D.; Dr. Kari Thyne; Command Sergeant Major John Labuz, USA (Ret.);*

*and Lieutenant Colonel Lukas Berg, USA, for their contributions to the advancement of ideas and emerging theses regarding joint special operations forces professionalism through their teaching and research on leadership, culture, and ethics as the professoriat of Joint Special Operations University.*

---

## Notes

<sup>1</sup> U.S. Special Operations Command (USSOCOM), *Comprehensive Review* (Tampa, FL: USSOCOM, 2020), available at <<https://sof.news/pubs/USSOCOM-Comprehensive-Ethics-Review-Report-January-2020.pdf>>.

<sup>2</sup> Andrew Abbott, *The System of Professions* (Chicago: The University of Chicago Press, 1988).

<sup>3</sup> *The Holloway Commission Report* (Washington, DC: The Joint Staff, 1980), available at <<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB63/doc8.pdf>>.

<sup>4</sup> Abbott, *The System of Professions*, 2, 91–96.

<sup>5</sup> Colin Furness, “The System of Professions,” *Education for Information* 35, no. 3 (August 2019), available at <<https://content.iospress.com/articles/education-for-information/efi190271>>.

<sup>6</sup> Abbott, *The System of Professions*.

<sup>7</sup> Furness, “The System of Professions.”

<sup>8</sup> *Ibid.*, 102.

<sup>9</sup> Abbott, *The System of Professions*, 40–52.

<sup>10</sup> USSOCOM, *Comprehensive Review*.

<sup>11</sup> *Ibid.*

<sup>12</sup> For further reference, see Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (New York: Belknap Press, 1981), 8–10; James Burk, “Expertise, Jurisdiction, and Legitimacy of the Military Profession,” in *The Future of the Army Profession*, ed. Don M. Snider and Lloyd Matthews (Boston: McGraw-Hill Custom Publishing, 2005), 43–44; Magali S. Larson, *The Rise of Professionalism: A Sociological Analysis* (Berkeley: University of California Press, 1979), 208.

<sup>13</sup> Don M. Snider, “The Army Profession and Ethic,” symposium presentation, Command and General Staff College Ethics Symposium, Center for the Army Profession and Ethic, December 4, 2012, available at <<https://www.slideserve.com/esben/the-army-profession-and-ethic-the-center-for-the-army-profession-and-ethic-04-dec-12>>.

<sup>14</sup> Isaiah Wilson III and Michael J. Meese, “Officership and the Profession of Arms in the 21<sup>st</sup> Century,” in *Fundamentals of Military Medicine*, ed. Francis G. O’Connor, Eric B. Schoomaker, and Dale C. Smith (Fort Sam Houston, TX: Office of the Surgeon General, 2019).

<sup>15</sup> Isaiah Wilson III and Scott Smitson, “Solving America’s Gray-Zone Puzzle,” *Parameters* 46, no. 4 (Winter 2016), 65.

<sup>16</sup> Furness, “The System of Professions.”

<sup>17</sup> Isaiah III Wilson, *Learning Pathways-in-Action*, White Paper No. 6 (Tampa, FL: Joint Special Operations University, 2021).

<sup>18</sup> Lew Irwin, “JCS Vision and Guidance for PME & Talent Management and Optimizing Joint Leader Development” PowerPoint, October 23, 2019, available at <[https://www.jcs.mil/Portals/36/Documents/Doctrine/MECC2019/mecc2019day1brief2jcs\\_vision\\_guidance\\_rev5.pdf?ver=2019-10-21-092954-007](https://www.jcs.mil/Portals/36/Documents/Doctrine/MECC2019/mecc2019day1brief2jcs_vision_guidance_rev5.pdf?ver=2019-10-21-092954-007)>.

<sup>19</sup> Isaiah Wilson III and Scott A. Smitson, “The Compound Security Dilemma: Threats at the Nexus of War and Peace,” *Parameters* 50, no. 2 (Summer 2020), available at <[https://ssi.armywarcollege.edu/wp-content/uploads/2020/05/Parameters\\_50-2\\_Summer-2020-Wilson.pdf](https://ssi.armywarcollege.edu/wp-content/uploads/2020/05/Parameters_50-2_Summer-2020-Wilson.pdf)>; “Compound Security as a Theory of Next with Dr. Isaiah ‘Ike’ Wilson III (Part 1 of 4),” February 18, 2021, video, 10:33, available at <<https://www.youtube.com/watch?v=IAqumzNrJtM&list=PLDdkXV7z6CqO2BysAi5sQyc4-W5LJlJ8>>.

<sup>20</sup> *SOF for life* is a common referent across the special operations communities connotating formal transition of the Active-duty special operations forces member (that is, on separation or retirement from Active service). And despite no longer being “licensed to practice” as a formal special operations professional, the member is still regarded as a lifelong part of the profession.

<sup>21</sup> Kuang-Ming Kuo, Paul C. Talley, and Chi-Hsien Huang, “A Meta-Analysis of the Deterrence Theory in Security-Compliant and Security-Risk Behaviors,” *Computers & Security*, vol. 96 (September 2020), available at <<https://www.sciencedirect.com/science/article/pii/S0167404820302042>>.

<sup>22</sup> S.L.A. Marshall, *The Armed Forces Officer* (Washington, DC: Department of Defense, 1950), 6, available at <[https://www.usna.edu/Ethics/\\_files/documents/SLA%20Marshall%20Armed%20Forces%20Officer.pdf](https://www.usna.edu/Ethics/_files/documents/SLA%20Marshall%20Armed%20Forces%20Officer.pdf)>.





Navy divers assigned to Naval Special Warfare unit raise hooked ladder during training exercise at Silver Strand Training Complex, San Diego, California, January 23, 2022 (U.S. Navy/Alex Perlman)

# What Is JSOU? Then, Now, and Next

By David M. Dudas, Bethany Fidermutz, and Amie Lonas

The Joint Special Operations University (JSOU) was formally organized in 2000 as a Department of Defense applied learning educational activity modeled after corporate universities. JSOU’s mission is to prepare special operations forces (SOF) professionals to address strategic and operational challenges, arming them with the ability to think through

problems with knowledge, insight, and foresight. JSOU’s genesis came only 8 months before the tragic events and watershed moment of September 11, 2001. The events of 9/11 signified a threshold crossing for the United States, the international community, and pointedly for joint-combined SOF. It has marked a 20-year-long focus on direct action and crisis response “anti-” and “counter-” missions.

JSOU’s charter is to serve as the U.S. Special Operations Command (USSOCOM) academic center of excellence for special operations studies and

research. JSOU is designed to create, promote, and sustain postsecondary scholarship through teaching, research, and outreach in the strategic and operational art of joint special operations. The university is organized to facilitate U.S. Code Title 10 responsibilities of the USSOCOM commander to prepare SOF to carry out assigned missions and to increase the combat readiness of the force. This is accomplished by conducting specialized education that is unique and peculiar to SOF and not normally offered in other professional military education (PME) programs.

---

Colonel David M. Dudas, USA (Ret.), Ph.D., is Senior Advisor for Horizon Strategies. Dr. Bethany Fidermutz is an Education Consultant. Dr. Amie Lonas is Dean of Faculty and Academic Affairs at Joint Special Operations University.



U.S. Special Forces and Egyptian airborne forces prepare to breach door upon entering Military Operations in Urban Terrain village during culmination exercise of Joint Combined Exchange Training in Cairo, Egypt, August 31, 2021 (U.S. Army/Daisy Bueno)

## JSOU NEXT Purpose and Priorities

With its inception in the summer of 2020, JSOU “NEXT” established and executed priorities aligned with the USSOCOM commander’s guidance to assess the university’s direction and current curriculum after 60 days—in short, a JSOU NOW assessment and initial aspects of a plan of action toward realizing JSOU NEXT. The areas of focus identified included:

- reconsidering what, how, and to which audience JSOU currently teaches
- focusing on the “first principles” and nesting with 2018 National Defense Strategy priorities, while being agile and innovative to anticipate and address future challenges<sup>1</sup>
- looking for divestitures and consolidations and reducing redundancy for greater cost-effective savings
- considering new delivery methods for teaching, curriculum modularity, core versus noncore, and cross-functional and cross-domain modules.

Now in its 21<sup>st</sup> year, JSOU is poised to address the unique character of the strategic and operational environments

that is marked by yet another threshold crossing of compound security threats in the context of strategic competition and irregular warfare. At its core, JSOU NEXT’s charge is to learn from the past to be more capable and ready in the future. This means analyzing SOF’s previous ages from their beginning in World War II, their role during the Cold War, SOF in the post-9/11 context of action, and what these previous stages present for requisite expert knowledge needed to address the challenges of strategic competition and to see future applications of SOF for the Nation, while learning from and avoiding past injuries.



Strategic competition in a joint environment is what SOF were born and bred to do. No single effort or suite of technology solves the puzzle of SOF's future use and utility for the achievement of national imperatives. Rediscovering the full continuum of SOF utility in strategic competition is the grounding imperative driving JSOU NEXT reforms and refits. The key to educating SOF to gain the advantage for the Nation's power purposes is to facilitate strategic and operational as well as critical and creative thinking in innovative ways. This ability includes enabling knowledge and practical

applications of special operations that defend and deter against adversaries' disruptor playbooks below thresholds of armed conflict through credible presence and preparedness of compelling force. Education provides the framework and multiple lenses through which we view and interpret the many aspects of a changing world. Without this understanding, we cannot assess threats and opportunities in ways that produce precise and actionable intelligence, and without awareness, we will target technologies as small fixes rather than a suite of synergistic tools that provide effect and agility in operations.

JSOU NEXT's educational design includes three primary lines of effort that are centered on teaching and learning, research and analysis, and service and outreach—all in the context of great global disruption, where threats are compounding at a rate that requires aligning ideas and resources in a manner that can overmatch these threats. For SOF to be at the leading edge of creating solutions for compound security dilemmas, it is imperative that JSOU set the right purposes, priorities, concepts, pillars, key tasks, main (big) ideas, and building blocks of success and organize the many ideas and concepts in



Army Green Berets assigned to 1<sup>st</sup> Battalion, 1<sup>st</sup> Special Forces Group (Airborne), observe target for Navy Sikorsky HH-60 helicopter during Close Air Support Training, Okinawa, Japan, May 13, 2021 (U.S. Army/Caleb Woodburn)

powerful ways, where SOF leader operators can transpose the expert knowledge acquired in the classroom to real-world practical applications.

Being at the leading edge requires understanding the purpose for JSOU today and in tomorrow's historical contexts of action—the need to achieve intellectual overmatch against our adversaries and competitors. To achieve this overmatch, JSOU NEXT's priorities start with adopting leading-edge techniques and research-based best practices in its learning models and methods. This includes modular delivery of an effective and agile outcomes-based curricula delivered both synchronously and asynchronously via resident, distant, and hybrid learning platforms; leveraging the latest technology; and incorporating andrological best practices in the physical

and virtual classroom with real-time assessment of intended learning outcomes. JSOU NEXT teaching includes a series of hubs with partnered civilian academic institutions, think tanks, government, and private industry across the United States and globally. These efforts are already having an impact on how we are thinking anew about curriculum design and delivery and how we can leverage research with other key stakeholders to influence the environment and build scholarship with strategic and operational impact.

Key to the initiative within JSOU NEXT is the development of an outcomes-based military education approach aligned to the Chairman's Desired Leader Attributes.<sup>2</sup> At the institutional level, JSOU has identified six overarching learning outcomes in support of

JSOU's goal to produce highly educated, hyper-enabled, responsible operators (better known by the acronym HE<sup>2</sup>RO). Specifically, JSOU graduates will:

- demonstrate advanced cognitive and communication skills employing agile, critical, creative, systematic, and innovative thought
- appreciate SOF as a *profession of arms* to include the embodiment and enforcement of shared ethics, norms, and laws
- apply knowledge of the nature, character, and conduct of special operations, war and conflict, and the instruments of national power across the full continuum of cooperation, competition, conflict, and war to achieve national security objectives
- generate threats and opportunities endemic to the current and future

operating environment based on analysis of historical, cultural, political, military, economic, technological, and other competitive forces

- design strategies and plans for the conduct of joint-combined SOF warfighting at the operational to strategic levels across the continuum of cooperation, competition, conflict, and war
- demonstrate the application of U.S., SOF, allied, and partner military force to conduct globally integrated, all-domain operations and integrative campaigns for national power purposes.

As a cognitive force multiplier in support of the Campaign Plan for Global Special Operations, JSOU has identified five mutually reinforcing learning pathways or integrated programs of study/discipline in addition to its Enlisted Academy—all emerging from the 2020 internal curriculum refit study:

- strategic influence and informational advantage
- strategic intelligence and emergent technology
- compound security threats in strategic competition
- SOF leadership and the SOF professional ethos
- resilience and resistance.

These pathways illuminate and advance learning in five identified joint SOF common core knowledge competency arenas and support the JSOU institutional learning outcomes (ILOs). The metaframe uniting these pathways is the focused set of SOF-unique core activities USSOCOM possesses that can be employed to gain irregular warfare asymmetric and informational advantages over competitors and adversaries across the entire competition continuum, with special focus on gray zones.<sup>3</sup>

Each pathway has unique program learning outcomes (PLOs) nested within the ILOs along with requisite subordinate learning outcomes needed for ultimate achievement of the PLOs. JSOU identified specific and measurable learning outcomes that are crosswalked across lesson, module, course, program, and institutional levels. The programs of

study cover a broad array of knowledge including 21<sup>st</sup>-century strategic influence and information advantage, strategic intelligence and emergent technology that enables and informs at the strategic-operational level, advanced application of resistance and resilience theory, design-based integrative statecraft, and ethically sound leadership and decision-making concepts and methodologies. The students who journey along these pathways will serve as enterprise future experts and thought leaders whose knowledge competencies will benefit current and future joint, interagency, interorganizational, and multinational cross-functional efforts across the spectrum of cooperation, competition, conflict, and war.

### JSOU NEXT and SOF's Grand Utility for the Nation

Growing, fostering, preserving, and sharpening the edge of SOF for the Nation is all about talent and leader development through PME that is governed by understanding the security environment and the contributions of all instruments of power. JSOU NEXT seeks to create SOF leader operators with the ability to anticipate and respond to surprise and uncertainty while leading through transitions on intent, trust, empowerment, and understanding. This includes making ethical decisions based on the shared values of the profession of arms and thinking critically and strategically in applying joint SOF warfighting principles and concepts to joint, interagency, intergovernmental, multinational, and commercial/civilian operations. To do this, JSOU will leverage inputs from the right leaders, experts, and practitioners in SOF and related fields.

JSOU NEXT seeks to provide PME that illuminates SOF's grand utility and its multiple, discrete capabilities that are uniquely suited to the geostrategic environment. JSOU seeks to empower the SOF enterprise to be the "first three feet" of the space where threats and interests come together, embodying the iron triangle of SOF as diplomat-sentinel-warrior.<sup>4</sup> Anticipating and avoiding strategic surprise is an imperative now more than

ever, and the empowered SOF operator can truly be the watcher on the wall when the risks we face are ever morphing, gray, and evolving. This means having strong connectivity to SOF commands; knowing policy decisions, direction, and strategic guidance; and taking full advantage of being near the flagpole, which is another way JSOU differentiates itself from other more conventional educational institutions. This strong connectivity means JSOU can also help decisionmakers be better commanders—addressing some tough, highly relevant questions or problems with USSOCOM, Joint Special Operations Command, and Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict collaboration. JSOU, therefore, seeks to play a unique role in helping to link U.S. national security interests and objectives to SOF capabilities at all levels. JFQ

---

### Notes

<sup>1</sup> *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>>.

<sup>2</sup> Chairman of the Joint Chiefs of Staff Memorandum CM-0166-13, *Desired Leader Attributes for Joint Force 2020* (Washington, DC: The Joint Staff, 2013), available at <[https://www.ndu.edu/Portals/59/Documents/BOV\\_Documents/2014/CJCS%20Joint%20Education%20Review%20Implementation%20Memo%20only.pdf](https://www.ndu.edu/Portals/59/Documents/BOV_Documents/2014/CJCS%20Joint%20Education%20Review%20Implementation%20Memo%20only.pdf)>.

<sup>3</sup> *Summary of the 2018 National Defense Strategy, NDS Irregular Warfare Annex* (Washington, DC: Department of Defense, October 23, 2019), available at <[https://www.jcs.mil/Portals/36/Documents/Doctrine/MECC2019/mecc2019day1brief8\\_iw.pdf?ver=2019-10-17-143158-750](https://www.jcs.mil/Portals/36/Documents/Doctrine/MECC2019/mecc2019day1brief8_iw.pdf?ver=2019-10-17-143158-750)>.

<sup>4</sup> The iron triangle of special operations forces as diplomat-sentinel-warrior is part of an ongoing study of SOF as a profession, originally conceptualized by David M. Dudas and Isaiah Wilson III.



Members of China's People's Liberation Army attend flag-raising ceremony at Tiananmen Square, in Beijing, China, June 16, 2021 (Reuters/Tingshu Wang)

# Persistent Knowledge Gaps in the Chinese Defense Budget

By Frederico Bartels

The People's Republic of China (PRC)'s People's Liberation Army (PLA) presents the most significant military challenge to the United States and its allies. It is therefore imperative for us to understand PLA funding to enhance our understanding of the role of the military instrument

---

Frederico Bartels is a Senior Policy Analyst for Defense Budgeting in the Davis Institute for National Security and Foreign Policy at the Heritage Foundation.

in PRC foreign policy. This article discusses the current knowledge of how much funding is available for the PLA and the gaps in that knowledge, some solutions that attempted to close these gaps, and some areas prime for further development. The cost of a military for a society is not only a theoretical question; it also reveals part of the relative importance of the military in that society. In the case of the PRC, many unknowns remain regarding the cost of the PLA. Such murkiness is expected:

The ruling Chinese Communist Party (CCP) constructed a notoriously ambiguous government in which members manipulate statistics and facts to fit its desired narrative.<sup>1</sup> When it comes to disclosing to the international community its military expenditures, CCP leadership announces a single figure on its defense budget annually. This figure falls short of what other countries release publicly and does not tell the whole story or reveal the whole amount that is dedicated to national defense.

This lack of transparency would be simply a nuisance if the CCP did not represent a fundamental challenge to the current rules-based international order and, increasingly, a rival to the United States.<sup>2</sup> In its 2017 National Security Strategy and 2018 National Defense Strategy, the Federal Government recognized and prioritized the threat China poses.<sup>3</sup> Furthermore, the Joseph Biden administration acknowledges the growing aggression of the PRC.<sup>4</sup> The 2018 National Defense Strategy describes a multipronged approach to exercising power and influence in the Indo-Pacific region, stating that “China is leveraging military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to [its] advantage.”<sup>5</sup> Much has been written and documented about the military modernization on which the CCP has embarked.<sup>6</sup> Because there is no documented internal domestic clamor for more data on the Chinese defense budget, however, international actors will have to produce the information. But persistent gaps in Western understanding of Chinese military expenditures and its defense budget—the inputs that enable PLA modernization processes—remain.

When compared with the effort dedicated to understanding Soviet military expenditures, current U.S. attempts to understand Chinese military expenditures are clearly still in their infancy. Noel Firth and James Noren, two former Central Intelligence Agency analysts, have detailed the robust internal debates that took place in the Federal Government on how to account and estimate the Soviet defense budget during the Cold War.<sup>7</sup> Multiple organizations studied and made informed judgments on how the Soviet defense budget was composed and how it compared with the U.S. defense budget. There were even so-called unconventional approaches that used industrial production data and other inputs to present a more precise estimate of the Soviet defense burden.<sup>8</sup> Barry Watts, former director of Program Analysis and Evaluation at the Pentagon, describes making different attempts to

estimate Soviet defense spending as one of the core tasks necessary to develop net assessments outlining the comparative advantages of different countries.<sup>9</sup> Although such methodologies had shortcomings, a discussion of them should shed light on military expenditures in totalitarian societies. Furthermore, these methodologies did bring a better understanding to how the Soviet military was organized and resourced. They also demonstrated that, as disclosures have shown, not even contemporary Soviet leaders knew the actual level of their military expenditures.<sup>10</sup>

These public discussions about the Soviet defense budget represent a level of detail that currently is not available on the Chinese defense budget. They demonstrate that the Federal Government used to have the analytical capability for these debates and to produce the data required for them. But today it is fair to assume that the Intelligence Community has had some of the discussion necessary to reach independent assessment of the Chinese defense burden. That said, only a few pages are made public through the annual China Military Power report produced by the Department of Defense.<sup>11</sup>

### Existing Data on the PRC Defense Budget

As of this writing, two sources in the English-language literature can be considered primary data on military expenditures of the PRC: the United Nations (UN) military spending database<sup>12</sup> and the 2019 China white paper on national security, *China’s National Defense in the New Era*.<sup>13</sup> These two sources present the same information, self-reported by the Chinese government, which like most Chinese data should be understood in the context of the CCP’s regime—that is, it contains only kernels of truth. In fact, the white paper lists the source for the budgetary data as “data on China’s defense expenditure submitted to the UN by the Chinese government.”<sup>14</sup>

This defense expenditure information submitted to the UN can be found in the UN Report on Military Expenditures, under the Office for Disarmament Affairs—an entity that started in 1980 as a mechanism to build confidence between

nations and promote transparency in military expenditures. The overall concept is that by bringing more attention and transparency to how states allocate their military resources, countries could have a better understanding of one another’s activities and thus potentially restrain military actions based on misperceptions. As with most UN efforts, the military expenditures database relies on the cooperation of the member states to provide data. There is a lack of consistency, however, that is reflected in gaps spanning years in each country’s report and by changes where the data are located within the UN Web site. Furthermore, this self-reporting approach means that the data are only as reliable as the country generating them wants them to be.

UN member states choose one of four forms with increasing levels of detail to report their annual military expenditures. The first is for countries that do not report any military expenditure. The other three involve different levels of detail for countries that do report military expenditures. The simplest form is a “single figure” report in which the country reports only a single figure reflecting their ministry of defense equivalent. Then there is the simplified form, which divides total military expenditure in two ways.<sup>15</sup> First, it divides the funding by the type of expenditure: personnel, operations and maintenance, procurement and construction, and research and development (R&D). Then, it categorizes those resources by which force controls them: land, naval, air, or other forces. The final form, which is the one recommended by the UN, builds on the simplified form.<sup>16</sup> For the type of expenditures, the form includes 28 categories that are nested under the 4 categories of personnel, operations and maintenance, procurement and construction, and R&D. The force side is split into 10 categories, including the different forces and elements such as support and command, UN peacekeeping, and emergency aid to civilians.

The voluntary reports submitted by the PRC are a half-filled version of the simplified form.<sup>17</sup> This level of disclosure falls short of what would be reasonable to expect from a responsible actor in the

international arena—especially one that is leading the world in military expenditures. The data do not report any resources allocated to R&D. In the category of forces, the report is divided into active, reserve, and militia components, instead of land, naval, and air forces as prescribed by the UN. These major departures from the form make it impossible to observe how PRC resources have changed.

The CCP's defense white paper uses these reports from 2010 to 2017 to construct a table showing the evolution of Chinese defense expenditures.<sup>18</sup> Even with the table's limited data, it is possible to observe that the CCP's defense expenditures nearly doubled in 8 years. Moreover, the table confirms a substantial increase in the percentage of military resources dedicated to purchasing equipment, growing from 33 percent of the budget to 41 percent. This boost indicates that significant resources are behind the PLA's rhetorical emphasis on modernization.<sup>19</sup> For a document that claims to reflect "reasonable and appropriate defense expenditure," however, it fails to provide information on how those expenditures are reasonable and appropriate.<sup>20</sup> The level of transparency demonstrated in the white paper is no different from that of the previously released UN-based data.

Also, just like the data available through the UN, the white paper addresses nothing on the past 4 years, from 2018 to 2021. Public reports give reason to believe substantive increases in the PRC's defense budget have occurred.<sup>21</sup> The United States and its allies should exert public pressure for the PRC to resume reporting under the UN mechanism. Even if these sources cannot be taken at face value, they represent a valuable data point that can and should be used for analysis.

### Limitations of the Current Data

The CCP has a worldwide reputation for manipulating and withholding data; in terms of defense budgets, it follows its regular playbook: being as opaque as possible. Transparency International UK, an anticorruption nongovernmental organization, developed a ranking to evaluate the transparency of countries'

defense expenditures, ranging from 0 to 12.<sup>22</sup> In that ranking, the PRC scored 1.5 out of 12, a "low" level of transparency. It is in this context of opacity that the primary source data must be evaluated and understood—that is, the figures should be taken with a grain of salt. Such skepticism does not eliminate the utility of or make invalid these data—rather, the data simply demand caution and caveats.

The lack of service-level information makes it difficult to determine how the PLA armed forces have changed through time, especially over a period when the PLA has been undergoing substantial reforms. The PLA has rebalanced its different forces, deemphasizing the role of the land forces, which have been dominant since the army's inception.<sup>23</sup> The UN form requires a breakdown between the different forces, but the PRC did not provide it. Another element of opacity is the short time frame of 8 years between 2010 and 2017 that is accounted for in the form. The small window provided makes it challenging to get a sense of the evolution of the PLA. Also, it is a somewhat outdated snapshot, already 4 years old as of this writing.

Further increasing the opacity of the data are the known omissions inside the budget. Funding devoted to R&D is the glaring omission. The UN reports require separate line items for military R&D resources; however, the PRC claims that "equipment expenses cover research and development, procurement, maintenance, transportation and storage of weaponry and equipment."<sup>24</sup> Such a claim is neither credible nor verifiable. At a minimum, it would be a step toward greater transparency for the Chinese government to report the funds allocated within each of the categories that compose "equipment."

Additionally, because of how the CCP defines the relationship between military research and the broader Chinese society, disclosing military, R&D funds would still give an incomplete picture. Under the civil-military fusion model that the CCP employs, the PLA can easily access for military purposes any technology and research developed in civilian

institutions.<sup>25</sup> As stated by Tai Ming Cheung, a professor at the University of California, San Diego, "Funding for defense-related research and development . . . comes primarily from other areas of the central government budget, most notably those allocated to the State Administration for Science, Technology, and Industry for National Defense (SASTIND), which is not included in the official defense budget."<sup>26</sup> SASTIND represents a line of expenditure that is outside of defense, and there is no indication that the budget is aggregated to the reported totals.<sup>27</sup>

The presence of state-owned enterprises (SOEs) in the PRC further highlights the challenges in getting a complete picture of military R&D. The Chinese defense industrial base has changed in the past few decades, but SOEs still play a major role in defense.<sup>28</sup> The current defense budget provides no visibility into the work of SOEs in the defense industrial base and how much support they get—or do not get—through the official defense budget. Transparency International UK summarizes the state of Chinese defense budget data well, stating that "the little official defence budget information which is released by the Chinese government excludes any data on military R&D and infrastructure projects, strategic forces, and foreign acquisitions."<sup>29</sup>

### Challenges in Dealing with the Existing Data

Even in the context of the limited data available on the PRC's defense budget, other limitations make it hard to compare Chinese military expenditures with those of the rest of the world. The main obstacle is in establishing a common currency for making the comparisons. Simplistic comparisons rely on using a market exchange rate to reach a common currency, usually U.S. dollars. Market exchange rates are the price of one currency that would be necessary at that given moment to buy another currency. However, unless someone is buying just currency, those rates have little utility. These market exchange rate comparisons lead to misleading



statements, such as “the United States spends more on defense than [the next 10 countries] combined.”<sup>30</sup> It is a statement devoid of context, thus undermining its credibility. These comparisons ignore the fact that military expenditures are mostly conducted inside the country with local currency and that the labor market for the military, a huge cost driver for most militaries, is national.<sup>31</sup>

Several studies develop a comparison with better fidelity by utilizing purchasing power parity (PPP) data.<sup>32</sup> Economists developed PPP indexes to permit comparisons between different economies

that have similar products available.<sup>33</sup> The main goal is to be able to compare the cost of living in different nations using a common basket of goods. PPP indexes aim to be universal and thus do not consider the specificities of a basket of goods the military would buy. Ideally, a specific PPP index would be available based on a military basket of goods. The World Bank and the UN should assess the viability of developing such an index.

Professor Peter Robertson from the University of Western Australia developed an initial concept of a real military purchasing power database. As he explains,

“Since output prices are not observable, I develop an exchange rate based on relative military input costs using defense budget share data. For each country the defense sector PPP exchange rate is constructed as a Törnqvist index of unit military costs relative to the USA.”<sup>34</sup> Further study is necessary to both replicate Robertson’s results and update the numbers, as the study uses 2017 data.

### Working Around the Data Limitations

The main way to get a better understanding of the PLA’s defense budget



Boatswain's Mate Seaman Daniel Bello (left) and Seaman Emilio Hernandez scan for surface contacts from bridge wing of guided-missile destroyer USS Dewey, East China Sea, November 10, 2021 (U.S. Navy/Justin Stack)

is for other organizations to produce alternative estimates, but it is also important for the United States to explore different methodologies and different sources of data, both inside and outside the Chinese government. Additionally, the United States should elicit the cooperation of its network of allies to crowdsource better data on how the PLA is resourced and how it applies its resources. During the Cold War, the United States needed to better comprehend how the Soviet Union budgeted for its military and how it evolved through time. The focus on one clear potential adversary enabled the Federal Government to encourage arguments among different analysts and organizations on how to best calculate and count Soviet military expenditures.<sup>35</sup> These debates ranged from how to understand the cost of each system and the salaries of Soviet military personnel to the rate of production of military assets and all the possible details that could be extracted from a closed society.

Compared with the current effort to get reliable Chinese data, the attempt

to access Soviet information on how it budgeted for its military and how much it allocated to each part was considerably harder. During the Cold War, “two basic approaches for independently estimating Soviet military spending (and thereby testing the working hypothesis) rapidly emerged. One relied on exploiting pertinent available Soviet economic statistics. The second eschewed the use of Soviet statistics and instead employed a direct-costing technique of putting price tags on known and estimated Soviet military forces, programs, and activities.”<sup>36</sup> Largely thought of as a top-down description of the defense budget, the first method utilizes the overall economy and the burden of government to determine the amount of funds dedicated to military spending. It focuses on the inputs that go into the defense sector. The second method relies on the purchase price of existing military assets plus their annual upkeep costs to estimate a country’s military expenditures. It largely concentrates on the outputs the countries receive from their expenditures.<sup>37</sup> Both types of analysis have been partially conducted

on the PLA’s expenditures, and myriad efforts have been taken to describe the PLA’s new platforms and their capabilities.<sup>38</sup> However, most of these analyses do not add a cost element to the equation, making it challenging to build out an aggregated defense budget by totaling major platform costs. It is not a matter of choosing one method or the other; rather, analysts should assess how these approaches could complement each other to give the public and the Intelligence Community a more complete picture.

In the context of Great Power competition, the United States must, using all possible sources of information, secure a better understanding of how the CCP funds its military, how much money is dedicated to military R&D, and how well Chinese military personnel are compensated. The Defense Intelligence Agency (DIA) issues an annual report called *China Military Power*. Its latest edition, published in late 2019, contains a two-page discussion of the Chinese defense budget, which includes a graph that merely reproduces the official Chinese defense budget, converted through



Sailor aboard guided-missile destroyer USS *Milius* observes bilateral exercise with Japan Maritime Self-Defense Force ships, South China Sea, November 16, 2021 (U.S. Navy/RuKiyah Mack)



President Joe Biden meets with Chinese President Xi Jinping during virtual summit in Roosevelt Room of White House, November 15, 2021 (Abaca Press/Alamy/Sarah Silbiger)

market exchange rates and adjusted for inflation.<sup>39</sup> The text acknowledges the challenges of an independent valuation, stating that “estimating actual military expenses is difficult because of China’s poor accounting transparency and incomplete transition to a market economy.”<sup>40</sup> Exactly because it is difficult, the DIA should develop its own independent estimate and make it public, which would allow other actors to expand on it.

The U.S.-China Economic and Security Review Commission (USCC), an independent congressional commission charged with reviewing the National security effects of U.S.-China interactions, also publishes an annual report on the activities of the PRC. The 2019 edition discussed the Chinese defense budget and highlighted lack of transparency, stating that “China’s official budget is not transparent. Authoritative observers note that one cannot accept China’s official figures at face value due to Beijing’s provision of only top-line

numbers and omission of major defense-related expenditures, such as research and development and foreign arms purchases.”<sup>41</sup> The commission takes its analysis one step beyond that of the DIA and includes a graphic representation of the Chinese defense budget alongside two independent estimates performed by independent research organizations.<sup>42</sup> A participant partially addressed this issue at one public hearing held by the USCC.<sup>43</sup> But that is where the discussion ends in publicly available sources from the Federal Government.

The USCC uses the estimates of two international research organizations: the Stockholm International Peace Research Institute (SIPRI) and the International Institute for Strategic Studies (IISS). Beginning in 1997, SIPRI developed its own methodology to estimate the Chinese defense budget. SIPRI’s approach incorporates elements missing from the official budgetary data publicized by the PRC government.<sup>44</sup> A January 2021 report

from SIPRI updated its methodology and built on the elements that are part of the independent estimate.<sup>45</sup> Its estimate for the Chinese defense budget takes into account military expenditures that occur outside the official defense budget.<sup>46</sup> The methodology considers military R&D, costs for the militia and the People’s Armed Police, subsidies for SOEs, and earnings from the PLA’s economic activities and arms exports. As stated by SIPRI, “the estimates for the years 1997–2017 are based on publicly-available figures for official military expenditure and some other items, and estimates for other items based on Professor Wang’s methodology or other methods based on new information.”<sup>47</sup> The SIPRI data therefore try to fill in the gaps that the publicly available data present. It is a methodology analogous to the building-blocks approach used in past assessments of the Soviet defense budget in which the different elements of the force are examined to get a greater picture of military expenditures.



Lieutenant Louis Petro stands watch as tactical action officer in combat information center aboard amphibious dock landing ship USS *Germantown*, East China Sea, July 17, 2020 (U.S. Navy/Taylor DiMartino)

IISS takes a similar tactic, finding the budgetary categories not represented in the official budget and adding its estimates to them. In a recent report, IISS highlighted new categories that ought to be included in the calculation of the PLA budget to bring it closer to reality.<sup>48</sup> IISS includes the local budgets for the People's Armed Police and the expenses for the China coast guard. Both inclusions are supported by their recent additions to the Central Military Commission's command structure, effectively making them part of the military chain of command. These additions align with the 2015 reforms of the PLA and its changes in the military structure.<sup>49</sup> According to IISS calculations, these two additions amount to an extra \$10 billion to the PLA's budget—a substantial addition to a budget that IISS already estimates to be around \$200 billion. The IISS report also points out five other

areas that should be explored to obtain a more precise estimation of the Chinese defense budget, ranging from the costs to build artificial islands in the South China Sea to the operations and maintenance costs of the China coast guard and the expense of building aircraft carriers.

A recent report from the Heritage Foundation advanced a different way to compare and contextualize the Chinese defense budget.<sup>50</sup> The report reduces the level of details presented on the defense budget of the United States to the ones available on the PLA budget, to obtain an equivalent picture. Because the United States provides substantially more budgetary data, it is possible to reaggregate the data in the categories utilized by the PRC and exclude the elements not presented in the PLA's data. From there, it is possible to utilize both market exchange rates and PPP, when appropriate, to reach a common measurement.

Employing these techniques, the report estimates that the defense budget of the PRC had 87 percent of the purchasing power of the defense budget of the United States in 2017. The year selected was the last year in which available data from the PLA's budget were broken down in any detail.

All these reports are an important step toward getting more clarity on the real level of military expenditures in China; however, these estimates should be refined as new data become available and as the international community gathers new sources of information on China.

## Conclusion

To a large extent, defense budget transparency is an area in which the United States leads the world; the United States and other nations should publicly engage and push the PRC to meet a similar standard. The UN Military

Spending database is a great place to start creating this pressure, especially because it is a mechanism that the PRC utilized until 2017. This push would have to be part of a broader effort to get the Chinese to become more transparent—a significant change in behavior for them. As highlighted by Princeton University’s Aaron Friedberg,

*In recent years U.S. officials have pressed their Chinese counterparts to be more “transparent” about defense spending, but there is little expectation that these pleas will yield meaningful results. Even if Beijing were suddenly to unleash a flood of information, American analysts would regard it with profound skepticism, scrutinizing it carefully for signs of deception and disinformation. And they would be right to do so; the centralized, tightly controlled Chinese government is far better able to carry off such schemes than its open, divided, and leaky American counterpart.*<sup>51</sup>

The opacity of the CCP, combined with the inherent distrust that its authoritarian system generates, means that, for the time being, the United States, allied governments, and independent researchers and organizations must strive to develop their own estimates of the Chinese defense budget, if there is to be any improvement in the collective understanding of it. The difficulty and possible pitfalls are all the more reason to get more individuals invested in calculating the right answer rather than a reason to abandon the work and rely solely on those data the CCP chooses to disclose.

A more accurate picture of Chinese military expenditures is a necessary, but not sufficient, component in assessing the PRC’s defense capacities and capabilities. In many cases, it is more important to know that an adversary *has* a certain system rather than what that system *costs*. But when it comes to devising peacetime strategies that aim at putting the adversary in a position where the cost curve is unfavorable, knowing these costs is critical. In terms of China’s military budget, a better understanding will come only from independent analysis—both inside and outside the Federal Government. JFQ

## Notes

<sup>1</sup> A good example of this behavior is demonstrated in Vanessa Molter and Renee Diresta, “Pandemics & Propaganda: How Chinese State Media Creates and Propagates CCP Coronavirus Narratives,” *Misinformation Review* 1 (June 8, 2020), available at <<https://misinformationreview.hks.harvard.edu/article/pandemics-propaganda-how-chinese-state-media-creates-and-propagates-ccp-coronavirus-narratives/>>.

<sup>2</sup> Huiyun Feng and Kai He, “China’s Institutional Challenges to the International Order,” *Strategic Studies Quarterly* 11, no. 4 (Winter 2017), available at <[https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11\\_Issue-4/Feng.pdf](https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Feng.pdf)>.

<sup>3</sup> *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), available at <<https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>>; *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge* (Washington, DC: Department of Defense, January 2018), available at <<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>>.

<sup>4</sup> *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), available at <<https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>>.

<sup>5</sup> *Summary of the 2018 National Defense Strategy*, 2.

<sup>6</sup> An especially good example is Phillip C. Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington, DC: NDU Press, 2019), available at <<https://ndupress.ndu.edu/Portals/68/Documents/Books/Chairman-Xi/Chairman-Xi.pdf>>.

<sup>7</sup> Noel E. Firth and James H. Noren, *Soviet Defense Spending: A History of CIA Estimates, 1950–1990* (College Station: Texas A&M University Press, 1998).

<sup>8</sup> William Thomas Lee, *The Estimation of Soviet Defense Expenditures, 1955–75: An Unconventional Approach* (New York: Praeger, 1977).

<sup>9</sup> Barry D. Watts, “Net Assessment in the Era of Superpower Competition,” in *Net Assessment and Military Strategy: Retrospective and Prospective Essays*, ed. Thomas G. Mahnken (Amherst, NY: Cambria Press, 2020), 27–72.

<sup>10</sup> Firth and Noren, *Soviet Defense Spending*, 188.

<sup>11</sup> *Military and Security Developments Involving the People’s Republic of China 2020: Annual Report to Congress* (Washington, DC: Office of the Secretary of Defense, 2020), available at <<https://media.defense.gov/2020/sep/01/2002488689/-1/-1/1/2020-dod-china-military-power-report-final.pdf>>.

gov/2020/sep/01/2002488689/-1/-1/1/2020-dod-china-military-power-report-final.pdf>.

<sup>12</sup> United Nations (UN), Office for Disarmament Affairs, Military Expenditures database, available at <<https://milex.un-arm.org>>.

<sup>13</sup> *In Their Own Words: China’s National Defense in the New Era* (Beijing: State Council Information Office of the People’s Republic of China, July 2019).

<sup>14</sup> *Ibid.*, 39.

<sup>15</sup> UN, “United Nations Report on Military Expenditures—Reporting Forms: Simplified Form,” available at <[https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/convarms/Milex/Forms/en/MilEx\\_simplified\\_reporting\\_form\\_web.doc](https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/convarms/Milex/Forms/en/MilEx_simplified_reporting_form_web.doc)>.

<sup>16</sup> UN, “United Nations Report on Military Expenditures—Reporting Forms: Standardized Form,” download available at <[https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/convarms/Milex/Forms/en/Standardized\\_reporting\\_form\\_web.doc](https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/convarms/Milex/Forms/en/Standardized_reporting_form_web.doc)>.

<sup>17</sup> The latest version available is from 2017. See People’s Republic of China (PRC), “Instrument for Standardized International Reporting of Military Expenditures,” 2017, download available at <<https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/03/MilEx-2017-China.pdf>>.

<sup>18</sup> *China’s National Defense in the New Era*, 39.

<sup>19</sup> Caitlin Campbell, “China’s Military: The People’s Liberation Army (PLA),” Congressional Research Service, January 5, 2021, available at <[https://www.everycrsreport.com/files/2021-01-05\\_IF11719\\_96211994c0d7e0f24d3851b53ab4f4e0b0b686e5.pdf](https://www.everycrsreport.com/files/2021-01-05_IF11719_96211994c0d7e0f24d3851b53ab4f4e0b0b686e5.pdf)>.

<sup>20</sup> *China’s National Defense in the New Era*.

<sup>21</sup> Matthew P. Funaiole et al., “Understanding China’s 2021 Defense Budget,” Center for Strategic and International Studies, March 5, 2021, available at <<https://www.csis.org/analysis/understanding-chinas-2021-defense-budget>>.

<sup>22</sup> Mariya Gorbanova and Leah Wawro, *The Transparency of National Defence Budgets* (London: Transparency International UK, October 2011), available at <<http://curbingcorruption.com/wp-content/uploads/2018/07/Gorbanova-and-Wawro-2011-The-transparency-of-national-defence-budgets.pdf>>.

<sup>23</sup> Saunders et al., *Chairman Xi Remakes the PLA*.

<sup>24</sup> PRC, “Instrument for Standardized International Reporting.”

<sup>25</sup> Lorand Laskai, “Civil-Military Fusion and the PLA’s Pursuit of Dominance in Emerging Technologies,” *China Brief* 18, no. 6 (April 9, 2018), available at <<https://jamestown.org/program/civil-military-fusion-and-the-plas-pursuit-of-dominance-in-emerging-technologies/>>.

<sup>26</sup> Tai Ming Cheung, “Keeping Up with the *Jundui*: Reforming the Chinese Defense Acquisition, Technology, and Industrial System,” in Saunders et al., *Chairman Xi Remakes the PLA*, 586.

<sup>27</sup> Military R&D was one of the most challenging numbers to estimate when assessing Soviet military expenditures. See Central Intelligence Agency, “Analyzing Soviet Defense Programs, 1951–1990,” 1998, available at <[https://nsarchive2.gwu.edu/NSAEBB/NSAEBB431/docs/intell\\_ebb\\_009.PDF](https://nsarchive2.gwu.edu/NSAEBB/NSAEBB431/docs/intell_ebb_009.PDF)>.

<sup>28</sup> Zoey Ye Zhang, “China’s SOE Reforms: What the Latest Round of Reforms Mean for the Market,” *China Briefing*, May 29, 2019, available at <<https://www.china-briefing.com/news/chinas-soe-reform-process/>>.

<sup>29</sup> Gorbanova and Wawro, *The Transparency of National Defense Budgets*, 23.

<sup>30</sup> Peter G. Peterson Foundation, “U.S. Defense Spending Compared to Other Countries,” May 13, 2020, available at <[https://www.pgpf.org/chart-archive/0053\\_defense-comparison](https://www.pgpf.org/chart-archive/0053_defense-comparison)>. Last updated July 9, 2021.

<sup>31</sup> Rachel Zissimos and Thomas W. Spoehr, *Putting Defense Spending in Context: Simple Comparisons Are Inadequate*, Background Paper No. 3229 (Washington, DC: Heritage Foundation, July 12, 2017), available at <<https://www.heritage.org/defense/report/putting-defense-spending-context-simple-comparisons-are-inadequate>>.

<sup>32</sup> See, for example, Richard Connolly, *Russian Military Expenditure in Comparative Perspective: A Purchasing Power Parity Estimate*, CNA Occasional Paper (Arlington, VA: CNA, October 2019), available at <[https://www.cna.org/CNA\\_files/PDF/IOP-2019-U-021955-Final.pdf](https://www.cna.org/CNA_files/PDF/IOP-2019-U-021955-Final.pdf)>; and Frederico Bartels, *China’s Defense Budget in Context: How Under-Reporting and Differing Standards and Economies Distort the Picture*, Special Report No. 225 (Washington, DC: Heritage Foundation, March 25, 2020), available at <<https://www.heritage.org/asia/report/chinas-defense-budget-context-how-under-reporting-and-differing-standards-and-economies>>.

<sup>33</sup> *Purchasing Power Parities and the Real Size of World Economies: A Comprehensive Report of the 2011 International Comparison Program* (Washington, DC: World Bank Group, 2015), available at <<http://pubdocs.worldbank.org/en/142181487105157824/ICP-2011-report.pdf>>.

<sup>34</sup> Peter E. Robertson, *International Comparisons of Real Military Purchasing Power: A Global Database*, Economics Discussion Papers No. 19.13 (Perth: University of Western Australia, October 23, 2019), 20.

<sup>35</sup> Firth and Noren, *Soviet Defense Spending*.

<sup>36</sup> *Ibid.*, 11.

<sup>37</sup> This method can be extremely challenging and requires a substantial amount of detailed data on the systems that are being costed and on how that society operated.

See Gertrude Schroeder, “Soviet Reality Sans Potemkin,” in *Inside CIA’s Private World: Declassified Articles from the Agency’s Internal Journal, 1955–1992*, ed. H. Bradford Westerfield (New Haven, CT: Yale University Press, 1995), available at <<https://www.gwern.net/docs/economics/1968-schroeder.pdf>>.

<sup>38</sup> A good example of documentation of People’s Liberation Army capabilities is P.W. Singer and Ma Xiu, “China’s Missile Force Is Growing at an Unprecedented Rate,” *Popular Science*, February 25, 2020, available at <<https://www.popsi.com/story/blog-eastern-arsenal/china-missile-force-growing/>>.

<sup>39</sup> *China Military Power: Modernizing a Force to Fight and Win* (Washington, DC: Defense Intelligence Agency, 2019), 21, available at <[https://www.dia.mil/portals/110/images/news/military\\_powers\\_publications/china\\_military\\_power\\_final\\_5mb\\_20190103.pdf](https://www.dia.mil/portals/110/images/news/military_powers_publications/china_military_power_final_5mb_20190103.pdf)>.

<sup>40</sup> *Ibid.*, 20.

<sup>41</sup> U.S.-China Economic and Security Review Commission, *2019 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: U.S. Government Publishing Office, November 2019), 295, available at <<https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf>>.

<sup>42</sup> *Ibid.*

<sup>43</sup> Phillip C. Saunders, *A “World-Class” Military: Assessing China’s Global Military Ambitions*, Testimony Before the U.S.-China Economic and Security Review Commission, 116th Cong., 1st sess., June 20, 2019, available at <[https://www.uscc.gov/sites/default/files/Saunders\\_USCC%20Testimony\\_FINAL.pdf](https://www.uscc.gov/sites/default/files/Saunders_USCC%20Testimony_FINAL.pdf)>.

<sup>44</sup> Stockholm International Peace Research Institute (SIPRI), “SIPRI Estimates for China,” SIPRI Military Expenditure Database, available at <<https://www.sipri.org/databases/milex/sources-and-methods#sipri-estimates-for-china>>.

<sup>45</sup> Nan Tian and Fei Su, *A New Estimate of China’s Military Expenditure* (Solna, Sweden: SIPRI, January 2021), available at <[https://www.sipri.org/sites/default/files/2021-01/2101\\_sipri\\_report\\_a\\_new\\_estimate\\_of\\_chinas\\_military\\_expenditure.pdf](https://www.sipri.org/sites/default/files/2021-01/2101_sipri_report_a_new_estimate_of_chinas_military_expenditure.pdf)>.

<sup>46</sup> Shaoguang Wang, “Estimating China’s Defence Expenditure: Some Evidence from Chinese Sources,” *The China Quarterly* 147 (September 1996), 889–911.

<sup>47</sup> SIPRI, “Footnotes and Special Notes,” SIPRI Military Expenditure Database, n49, available at <<https://www.sipri.org/sites/default/files/Footnotes.pdf>>.

<sup>48</sup> Meia Nouwens and Lucie Béraud-Sudreau, *Assessing Chinese Defence Spending: Proposals for New Methodologies* (London: International Institute for Strategic Studies, March 2020), available at <<https://www.iiss.org/-/media/files/research-papers/assessing-chinese-defence-spending---iiss-research-paper.pdf>>.

<sup>49</sup> Saunders et al., *Chairman Xi Remakes the PLA*.

<sup>50</sup> Bartels, *China’s Defense Budget in Context*.

<sup>51</sup> Aaron L. Friedberg, *A Contest for Supremacy: China, America, and the Struggle for Mastery in Asia* (New York: W.W. Norton & Company, 2011), 42.



F-15C Eagle assigned to 48<sup>th</sup> Fighter Wing conducts aerial operations in support of Bomber Task Force Europe 20-2 over Keflavik, Iceland, March 16, 2020 (U.S. Air Force/Matthew Plew)

# U.S. European Command Theater Infrastructure Plan

## Aligning U.S. Requirements with European Capability and Resources

By Jon-Paul Depreo and Scott P. Raymond

U.S. European Command (USEUCOM) has had a long and storied history since 1952, providing response to more than 200

named operations including humanitarian and natural disaster relief efforts and deployed forces in support of nearly 95 contingency operations.<sup>1</sup>

As old threats become new threats, USEUCOM continues to sync with national strategy and develop plans that leverage existing and planned infrastructure investments throughout Europe to reverse post-Cold War posture reductions. In response to the 2014 Russian annexation of Crimea,

---

Lieutenant Colonel Jon-Paul Depreo, USA, is Commander of the 46<sup>th</sup> Engineering Battalion, Fort Polk, Louisiana. Captain Scott P. Raymond, USN, is Strategic Logistics Chief and Engineer at U.S. European Command.

USEUCOM and European allies increased their commitment to defense spending and refocused their forces and footprint to deter further Russian aggression; however, with the pivot to the Indo-Pacific region to address emerging Chinese threats—during a period of constrained investments—USEUCOM’s infrastructure strategy is at risk of not reaching full potential.

A national strategy underpinned by a coherent infrastructure plan would mitigate unintended consequences of historical pendulum swings in resourcing.

The 2018 U.S. National Military Strategy (NMS) acts as a framework for “protecting and advancing U.S. national interests” for the joint force, allowing it to maintain its military advantage and implement defense strategies.<sup>2</sup> The NMS

describes a ready position supported by three strategy horizons: force employment, force development, and force design. The strategy horizons range to 15-year visions, with emphases on critical infrastructure and “a joint force that can exercise assured force projection, maintain freedom of maneuver in all domains, deliver joint combined arms decisively, and ultimately win” in support



Two Airmen assigned to 31<sup>st</sup> Security Forces Squadron participate in exercise Steadfast Nomad 2021 at Aviano Air Base, Italy, September 22, 2021 (U.S. Air Force/Brooke Moeder)



of homeland defense and allied defense against regional and global threats.<sup>3</sup> Timely infrastructure development—offering flexibility and strategic options to the commander—is critical to the application of joint planning principles.<sup>4</sup>

In 2019, the need for a theater infrastructure plan (TIP) at the joint strategic level manifested from a multitude of reasons. General Tod Wolters, USAF, issued a command directive for convergence between USEUCOM and Supreme Headquarters Allied Powers Europe to create more coherence in theater operations, activities, and investments. A TIP would coalesce disparate military construction (MILCON) efforts and seek to offset reductions in that budget. When realized and fully implemented, the TIP would be a dynamic requirements-based document organizing infrastructure shortfalls that result from gaps between needs and existing theater capabilities. This plan would consolidate U.S. infrastructure requirements across the USEUCOM theater and enable unity of effort within the joint force. Most important, the TIP would converge plans and investments with our allies, partners, and European Union (EU) organizations. The USEUCOM operational environment, especially in Eastern Europe, proves too dynamic for effective infrastructure support from a lengthy MILCON process. The TIP would also contain a coherent plan that is adequately dynamic and flexible to meet today's needs and project long-term solutions for tomorrow's fight in support of U.S. military objectives. The TIP would make MILCON the option of last resort.

This article explores USEUCOM's conceptual framework for the TIP, which will support national military strategy, improve convergence with European allies and partners, and reduce risk to military mission and force. The adoption of a deliberate infrastructure planning strategy at the theater level should provide resource efficiencies and flexibility to reach desired conditions of securing the Euro-Atlantic region, achieving a competitive edge, supporting North Atlantic Treaty Organization (NATO) credible

deterrence and defense, and enabling U.S. global power projection.<sup>5</sup>

The TIP's coordination and synchronization with EU planning and resourcing advances USEUCOM's combat commander's campaign plan and reduces the risk of an insufficient support infrastructure in times of crisis.

### Supporting U.S. Strategic Objectives

The joint and multinational force emphasis on the transregional, multidomain, and multifunctional environment in operational planning strengthens Europe's defense. Over the past 5 years, USEUCOM operational plans have been refined to put more focus on military mobility, convergence with allies and partners, and new regional and global threats. To counter growing pressures from Russia and China, the Department of Defense and Congress provided billions of dollars for programs and initiatives to enhance U.S. and NATO readiness for rapid response to aggression; to strengthen infrastructure capacity and burden-sharing opportunities; and to increase equipment prepositioning and joint reception, staging, and onward movement throughput. USEUCOM continues to prepare the theater by enabling an environment for ingenuity and creative solutions. A coherent infrastructure plan offers the efficiency and coherence that safeguards U.S. investment and national objectives.

Neither the Joint Staff nor the Office of the Secretary of Defense (OSD) mandates that unified commands establish an infrastructure support plan for combatant command activities, operations, and investments; however, the Joint Strategic Capabilities Plan (JSCP) translates NMS and Global Employment of the Force guidance into strategic planning requirements for the command. The 2020 JSCP Logistics Supplement directs combatant commands to publish a theater posture plan, a theater distribution plan, and theater logistics overview, which in the aggregate constitutes a theater logistics plan.<sup>6</sup> Although all three theater logistics plan elements describe infrastructure development, none identifies

or effectively communicates the totality of USEUCOM's infrastructure gaps or shortfall resolution options across the joint force (including both organic and host-nation infrastructure assets) in support of the transregional, multidomain, and multifunctional environment. Furthermore, the posture plan focuses most of the reliance on internal U.S. investments within a near-term horizon. A coherent infrastructure plan with a 15-year vision is essential to giving the best military advice on infrastructure and flexibility to the commander.<sup>7</sup> A key aspect of the TIP is its complementary role to USEUCOM's theater posture plan, which is bound by the OSD's Future Years Development Program (FYDP). The TIP looks longer term—an additional 10 years beyond the FYDP—and deemphasizes MILCON due to budget volatility, which makes out-year programming inconsistent and USEUCOM susceptible to OSD reallocation in favor of other global requirements (such as U.S. Indo-Pacific Command's emerging Pacific Deterrence Initiative).

Long-term understanding beyond near-term planning presents new options to reduce Service component reliance on MILCON appropriations to fill such infrastructure gaps as munitions and fuel storage facilities, equipment prepositioning warehouses, and airfield improvements. USEUCOM must make MILCON a solution of last resort—by emphasizing the TIP's use of more cost-efficient, predictable, and responsive options to address the combatant commander's needs. A long-term vision for infrastructure should inform the commander's campaign plan strategy and the subsequent Service component supporting plans.

### Convergence with NATO and Partners

The NATO Defense Planning Process (NDPP) seeks to standardize and increase planning interoperability across all 30 nations. The NDPP aims to harmonize military planning efforts within the Alliance via a five-step process: establishing guidance, determining requirements, setting target apportion needs, facilitating implementation, and

reviewing results. The NDPP results in the recognition of a minimum capability requirement and the resulting shortfalls, development of higher level NATO objectives, and decisions to generate statements of requirement. The NDPP's demand signal informs the Common Funded Capability Delivery Model and, therefore, what receives common funding. The TIP would allow USEUCOM to provide its infrastructure needs to NATO to inform the NDPP. Infrastructure requirements transparency creates convergence and infrastructure coherence across the theater.

Financial support to NATO consists of indirect and direct funding. Indirect funding manifests, for example, as the voluntary contribution of equipment or troops. In 2006, NATO's defense ministers agreed to a 2 percent of gross domestic product national defense spending target, with 20 percent of that defense budget spent on major equipment. In 2014, heads of state and government at the Wales Summit approved this defense spending target declaration to reaffirm the "strong commitment to collective defence and to ensuring security and assurance for all Allies."<sup>8</sup> Direct funding finances, for requirements serving the interests of all 30 nations, use a cost-share formula based on gross national income. One of these common funded arrangements is the NATO Security Investment Program (NSIP). A long-term infrastructure investment program, NSIP funds construction and command and control systems to offer military capabilities that are beyond the needs of individual member nations. In recent years, annual NSIP investments have averaged €750 million (approximately \$851 million). Starting in fiscal year 2021 (FY21), the U.S. cost-share of the NSIP common funding requirement decreased from 22 percent to 16 percent (\$120 million per year).

The U.S. return on investment from NATO funding mechanisms—such as direct funding of U.S. infrastructure, NATO projects at U.S. operating locations, and general NATO efforts since 2016—is approximately €5 billion (approximately \$5.7 billion; 16 percent)

of the total €31 billion (approximately \$35.2 billion) authorized by NATO. NSIP infrastructure investments approved since 2016 span 25 nations and should be completed in the next 10 years. Approved NSIP projects of U.S. interest include infrastructure supporting fighters, air-to-air refueling, air transport, the Airborne Warning and Control System, bombers, and aerial surveillance; fuel storage and delivery; equipment prepositioning; training ranges; and reception, staging, and onward movement of forces. Historically, NSIP investment for U.S. projects has been achieved through a bottom-up approach focused on specific projects. To increase future benefits of NSIP project funding, the United States is transitioning to a top-down approach that integrates USEUCOM basing and infrastructure requirements into NATO defense planning and associated NATO capability program plans, which would better align NSIP and U.S. project development.<sup>9</sup> The TIP ensures that U.S. long-range infrastructure planning is in place to parallel NATO planning, thus better positioning the United States to insert needs into the NATO planning process that set medium- and long-term horizons from 7 to 20-plus years. The TIP coalesces USEUCOM infrastructure requirements in support of NATO's goal to improve readiness.

The European Union is made up of 27 nations—21 of which are NATO members—seeking "to continue prosperity, freedom, communication, and ease of travel and commerce for its citizens."<sup>10</sup> The EU sought to improve cooperation by establishing in December 2017 a treaty-based organization called Permanent Structured Cooperation. Participating nations pledge to bolster global cooperation on projects "responding to the EU priorities by EU member states through the Capability Development Plan, also taking into account the results of the Coordinated Annual Review on Defence."<sup>11</sup>

EU investments in the Trans-European Transport Network reflect a priority to improve and strengthen European infrastructure. From 2000 to 2006, the EU invested €859 billion

(approximately \$975.7 billion) in transportation-related infrastructure and will likely contribute €1.5 trillion (approximately \$1.7 trillion) between 2010 and 2030.<sup>12</sup> From an infrastructure development perspective, U.S. cooperation with the EU is important to open the aperture for U.S. infrastructure development and use options captured in the TIP.

## Reducing Risk in the USEUCOM Theater

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3105.01, *Joint Risk Analysis*, identifies two types of risk: strategic and military. *Strategic risk* includes those activities that would result in negative consequence to the homeland, national interests (including NATO), or the invasion or loss of an ally or partner.<sup>13</sup> *Military risk* encompasses risk to mission (inability to meet military objectives) and risk to force (inability to provide and sustain sufficient military resources).<sup>14</sup>

CJCSM 3105.01 subdivides risk to mission as operational risk and future challenges. Operational risk exists within the near term (0 to 2 years), and future challenges extend to the medium term (0 to 7 years).<sup>15</sup> As a result of the TIP's cohesive effect, USEUCOM planners have increased flexibility during course-of-action development. Due to lengthy planning, design, and construction timelines, USEUCOM's ability to reduce risk in the near and medium term must start with a long-term vision. The TIP improves risk analysis decisions by bringing into focus the totality of the infrastructure requirements and capabilities, which allows decisionmakers to target investments where they are most effective. Improving resiliency through the development of a network of theater infrastructure reduces risk to mission by investing in long-term infrastructure planning. The TIP ultimately reduces risks to USEUCOM plans via a long-term vision, alternate infrastructure solutions, and strengthened relationships with allies and partners.

USEUCOM underwent transformative change in 2014 with the inception of the European Reassurance Initiative, now known as the European Deterrence

Initiative (EDI), which came about in response to Russia's actions in Crimea and eastern Ukraine. EDI provides Service components the opportunity to program MILCON projects addressing infrastructure shortfalls, including \$2.6 billion of infrastructure improvement funding from FY15 through FY21; as of FY20, more than half (\$1.8 billion) was deferred due to an emergency declaration at the southern border of the United States. Starting in FY22, as EDI MILCON dwindles

and reverts to the Armed Forces' base budgets, USEUCOM risks having an improperly resourced mitigation strategy. Therefore, USEUCOM must seek innovative solutions for infrastructure shortfalls. Allocating resources to infrastructure development and sustainment reduces delays and loss of progress.

USEUCOM reduces risk to mission by continuing convergence with NATO and cooperating with partner nations. Bilateral agreements such as defense cooperation

agreements establish authorities for execution of MILCON and use of existing facilities; however, these agreements are at the policy level and in most instances do not support shared understanding within NATO. For instance, U.S. Navy Europe's maritime requirements in support of NATO plans in northern Europe are developed in direct coordination with each host nation. As a result of bilateral arrangement, the needs are classified and releasable only to the respective nation.



Paratroopers assigned to 3<sup>rd</sup> Brigade Combat Team, 82<sup>nd</sup> Airborne Division, wait to exit C-17 Globemaster III bound for Estonia during exercise Swift Response 21, May 7, 2021 (U.S. Army/Alexander Burnett)

The resulting inability to integrate the infrastructure requirements into the NDPP results in miscommunication and misalignment of national intentions and goals. The TIP will ensure that infrastructure needs stay at a level granting maximum transparency and collaboration.

USEUCOM's ability to "buy down" risk is becoming increasingly limited as EDI resourcing uncertainties, competing global threats to geographical combatant commands, and policy decisions challenge service budgets. The TIP provides military risk mitigation to theater objectives by optimizing resource planning, certifying infrastructure that is built fit for purpose, and improving resiliency through development of a robust network.

## Conclusion

USEUCOM's creation of the TIP, with a 15-year vision, ensures direct alignment with the NMS, operation plans, and the USEUCOM's combat commander's campaign plan's three lines of effort to compete, deter, and prepare. The TIP focuses well beyond the FYDP, allowing USEUCOM to coordinate guidance that creates efficiencies and maximizes returns on investments—allowing Service components to develop their programs in support of TIP guidance. USEUCOM's requirement to conduct integrated infrastructure planning promotes convergence with the NATO Allies and partners, which in turn allows for burden-sharing and a common understanding.

Now more than ever, the TIP is needed to "better align ends, ways, and means to maximize the probability that the nation will meet its targeted policy objectives."<sup>16</sup> The TIP provides convergence with U.S. joint infrastructure needs and allows wise resource decisions with NATO Allies and partner nations. The NSIP's \$750 million per year allowance presents an opportunity, when approached with a proactive mindset, to enhance plan development collaboration and coordination. By funding more than \$48 billion to support the development of the Trans-European Transport Network, the EU's Connecting Europe Facility is providing an opportunity to create

operational effects and achieve the U.S. national objectives described in the NMS.

U.S. MILCON should be the option of last resort within the USEUCOM theater. The decisive effects of a TIP are measured through generating potential cost savings; developing USEUCOM staff efficiency; increasing convergence and cooperation between U.S., NATO, and EU planning; and reducing military risk. USEUCOM's determination to offer diverse infrastructure sourcing solutions for the commander—through better cooperation with the EU, NATO, and host nations—mitigates risk within operational planning and crisis response options, enabling a decisive response.

USEUCOM's history demonstrates an ebb and flow of conflict with congruent resourcing. As national strategy continues to address global threats and balance resources, USEUCOM's infrastructure planning requires support, through alternate means, to minimize the effects of refocused resourcing. The TIP's realized effects ensure a coherent plan that is dynamic and flexible to meet today's needs for tomorrow's fight. JFQ

## Notes

<sup>1</sup> U.S. European Command (USEUCOM), "History of USEUCOM," available at <<https://www.eucom.mil/organization/history-of-useucom>>.

<sup>2</sup> *Description of the National Military Strategy* (Washington, DC: The Joint Staff, 2018), available at <[https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS\\_2018\\_National\\_Military\\_Strategy\\_Description.pdf](https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf)>.

<sup>3</sup> *Ibid.*, 9.

<sup>4</sup> According to Joint Publication 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), xiii, the principles of planning are: focused on the objective; globally integrated and coordinated; resource informed; risk informed; framed within the strategic environment and operational environment; informs decisionmaking; and adaptive and flexible.

<sup>5</sup> *Combatant Commander's Campaign Plan-20* (Stuttgart, Germany: USEUCOM, 2021), figure 3.

<sup>6</sup> Chairman of the Joint Chiefs of Staff Instruction 3110.03F (DRAFT), *Logistics Supplement for the Joint Strategic Campaign Plan* (Washington, DC: The Joint Staff, 2020), B-5.

<sup>7</sup> Fifteen years is a conceptual goal to bridge the time gap between a 5-year Fiscal Year Defense Plan and the 20- to 30-year strategic concepts discussed in the 2018 National Defense Strategy.

<sup>8</sup> North Atlantic Treaty Organization, "Wales Summit Declaration," press release, September 5, 2014, available at <[https://www.nato.int/cps/en/natohq/official\\_texts\\_112964.htm](https://www.nato.int/cps/en/natohq/official_texts_112964.htm)>.

<sup>9</sup> Commander's Campaign Plans are a programmatic approach for the coordinated management of a required capability to achieve the strategic benefits and objectives across all aspects of doctrine, organization, training, materiel, leadership (and education), personnel, facilities, and interoperability, as outlined in the NATO Operational Requirement Statement. Actions include the identification, rationalization, monitoring, and control of the interdependencies between projects as well as tracking the contribution of each project to the consolidated program benefits.

<sup>10</sup> Amanda Briney, "The European Union: A History and Overview," *ThoughtCo*, April 10, 2019, available at <<https://thoughtco.com/european-union-history-and-overview-1434912>>.

<sup>11</sup> "Deepening Defence Cooperation Among EU Member States," Permanent Structured Cooperation, November 2020, available at <[https://eeas.europa.eu/sites/default/files/pesco\\_factsheet\\_november\\_2020-v1.pdf](https://eeas.europa.eu/sites/default/files/pesco_factsheet_november_2020-v1.pdf)>.

<sup>12</sup> "Transport Facts & Figures," European Commission, updated April 16, 2020, available at <[https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/en/facts\\_and\\_figures.html](https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/en/facts_and_figures.html)>.

<sup>13</sup> Chairman of the Joint Chiefs of Staff Manual 3105.01, *Joint Risk Analysis* (Washington, DC: The Joint Staff, October 14, 2016), C-5.

<sup>14</sup> *Ibid.*, C-8.

<sup>15</sup> *Ibid.*, C-8.

<sup>16</sup> *Ibid.*, A-3.



Two U.S. Air Force F-35A Lightning IIs assigned to Hill Air Force Base, Utah, and two Dassault Rafales assigned to Saint-Dizier–Robinson Air Base, France, break formation during flight over France, May 18, 2021, as part of exercise Atlantic Trident 21 (U.S. Air Force/Alexander Cook)

# All Quiet on the Eastern Front

## NATO Civil-Military Deterrence of Russian Hybrid Warfare

By Andrew Underwood, Andrew Emery, Paul Haynsworth, and Jennifer Barnes

Major Andrew Underwood, USA, is Executive Assistant to the Deputy Director for Strategy, Plans, and Policy (J5), Europe, NATO, Russia. Colonel Andrew Emery, USAF, is the Space and Missile Defense Planner in the U.S. Military Delegation to the NATO Military Committee (JCS) at NATO Headquarters, Brussels, Belgium. Lieutenant Colonel Paul Haynsworth, USA, is currently serving in the Commander's Action Group in the NATO Special Operations Headquarters at Supreme Headquarters Allied Powers Europe, Mons, Belgium. Commander Jennifer Barnes, USN, most recently served in the Commander's Action Group at U.S. Africa Command Headquarters in Stuttgart, Germany.

Russia's 2014 invasion of and continued threats (and now active war) against Ukraine have forced the North Atlantic Treaty Organization (NATO) to acknowledge that the era of European territorial conquest has



Special tactics operators assigned to 352<sup>nd</sup> Special Operations Wing radio to Swedish C-130H during controlled landings and takeoffs in Sweden, November 9, 2020, to support bilateral exercise in Baltic Sea region (U.S. Army/Patrik Orcutt)

not ended. Despite its success at deterring Soviet aggression during the Cold War, NATO must evolve to effectively counter Russia's 21<sup>st</sup>-century model of illicit actions and activity against NATO members—often referred to as hybrid warfare. To achieve credible deterrence, NATO's policy and strategy instruments must focus on imposing costs on Russian adventurism and limiting the effectiveness of Russian hybrid warfare campaigns. The preparation of civil institutions and structures as part of deterrence warrants study. The Alliance should consider how future conflicts would likely manifest between NATO and Russia and how Allies and partners could collectively deny or decrease the benefits available to Russia through its hybrid warfare approach.

The term *hybrid warfare* (or *hybrid threats*) lacks a universally accepted definition,<sup>1</sup> and Department of Defense

terminology predates the 2014 invasion.<sup>2</sup> Hybrid warfare can include conventional and unconventional forces or be carried out by other state and nonstate actors. It occurs across the diplomatic, informational, military, and economic dimensions of power. It may be overt but is just as often covert or clandestine, complicating attribution. Rather than attempting a formal definition, for the purpose of this article hybrid warfare refers to all available means undertaken by a state—in this case, Russia—across all power dimensions, including through intermediaries, to achieve its objectives against an adversary in such a manner that does not give rise to traditional war.

Russia uses hybrid warfare (though it does not name it as such; the term originates in the West) to advance national objectives using means not typically considered clear acts of war to manipulate facts on the ground without provoking

external intervention.<sup>3</sup> It is, in effect, delivering a *fait accompli* before its adversaries can respond. For its part, the joint European Union (EU)–NATO European Centre of Excellence for Countering Hybrid Threats defines *hybrid warfare* as “an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means.”<sup>4</sup>

Effective deterrence and defense require credibility, capability, and communication.<sup>5</sup> Major NATO policy statements over the past decade from Warsaw, Wales, Brussels, and London mention “an appropriate mix of nuclear, conventional, and missile defence capabilities” as the primary components of the Alliance's deterrence posture.<sup>6</sup> Deterrence in this context should be considered in terms of cost and benefit—one could deter an adversary by increasing the costs for taking action, reducing the benefit of taking action,

or ideally both, to encourage adversary restraint. The 2019 London Declaration acknowledges the need to “prepare for, deter, and defend against hybrid tactics” but fails to articulate *how* the Alliance should proceed.<sup>7</sup> Since Russian hybrid warfare manifests in ways clearly distinct from direct armed conflict between states, the use of military means in response might be difficult to legitimize. Just as hybrid warfare has evolved, responses to hybrid warfare must evolve and expand into other domains.

Building on NATO’s work, thinking, and publications on countering hybrid/gray zone warfare, the analysis presented here provides a framework on the Soviet and contemporary Russian methods within the current operational environment. It then proposes specific actions that NATO must adopt to impose costs on or deny benefits to Russia for employing these tactics, while also encouraging Russian restraint against future hybrid warfare.

### Framework to Consider Russian Hybrid Warfare

Hybrid warfare is not a new concept for Russia. The Soviet use of special forces, secret police, KGB (*Komitet Gosudarstvennoy Bezopasnosti*, Committee for State Security) agents, and other means to create political influence, manipulate perceptions, and undermine the spread of democracy is well documented. President John F. Kennedy described the Soviet Union as a “tightly knit, highly efficient machine that combines military, diplomatic, intelligence, economic, scientific, and political operations.”<sup>8</sup> Similarly, in 2017, RAND identified six primary types of Russian hybrid activity: information operations, cyber, proxies, economic influence, clandestine measures, and political influence.<sup>9</sup> What the Cold War-era tactics highlighted by Kennedy captured is a blurred non delineation of norms and practices applied both internally and externally to achieve objectives. Moreover, these tactics continue to this day. This distinction among activities and domains remains novel to many (though certainly not all) of NATO’s members.

Russia leveraged ethnic Russians as deniable proxies to stoke instability in Estonia in 2007 while simultaneously conducting cyber attacks.<sup>10</sup> The next year, Russia encouraged separatism within South Ossetia and Abkhazia and surged mercenaries and volunteers into the region, before transitioning to open conflict as its “peace-keeping” force took direct action and conquered Georgian territory in August 2008.<sup>11</sup> Russia’s success in employing hybrid warfare tools perhaps emboldened the state to undertake a grand-scale, near-seamless synchronization of hybrid activity that ultimately achieved the objectives of seizing and integrating Crimea and introducing a contested battleground within eastern Ukraine in 2014. Russia’s comprehensive hybrid campaign was as successful on the battlegrounds of Crimea and south-eastern Ukraine as it was in winning within the international rules-based order. Despite the objections of the plurality of nations, Crimea remains under Russian political control today, the contested area in eastern Ukraine remains a warm frozen conflict (which Ukraine refers to as the Anti-Terrorist Zone), and the threat of broader armed Russian incursion remains.<sup>12</sup>

During the Cold War, the Soviet Union employed hybrid warfare as a tool of global power competition to further the ideological struggle between communism and capitalism. Russia’s contemporary use of these operations is not as easily linked with an ideological narrative. Some argue that Russian actions are driven by President Vladimir Putin’s desire for other nations—and especially the United States—to acknowledge and respect Russia.<sup>13</sup> Others contend that NATO member expansions, activities, and partnerships threaten Russia.<sup>14</sup> Russian activity and objectives likely cover the gamut of Putin’s international and domestic priorities, from Moscow to the former Soviet states, to all of Europe and around the globe.

As the greatest power among the former Soviet states and the Soviet Union’s geopolitical successor, Russia wants to retain regional influence and be the region’s preeminent partner over others, such as the EU or the United States. When many of these states aligned with

NATO or the EU in the post-Cold War era, it was as much a rejection of Russia’s influence as it was a threat to Russia’s geopolitical future. Estonia, Georgia, and Ukraine have suffered Russia’s hybrid retaliation in response.

Russia’s desire for legitimacy as a Great Power extends beyond its “near abroad” into the rest of Europe and around the world. Despite shared heritage with many European nations, Russia’s frequent rejection of Western norms has kept Europe from fully embracing post-Cold War Russia into its clique. Exacerbating this gulf, Russia uses its hybrid muscle to undermine the European rules-based institutional framework.<sup>15</sup> It focuses its hybrid energies to ensure Russian operations can continue unconstrained by the European Union while attempting to fracture the NATO alliance. The invasion of Ukraine was a masterstroke at asserting its Great Power status, challenging the European security architecture, and demonstrating the impotence of the rules-based international order in constraining its actions.

Russia’s objectives appear to be to cement its own internal political legitimacy through restoring its international prestige as a Great Power, asserting regional influence across Europe, and undermining liberal Western democratic institutions. Russian threats of broader conflict or actions might indicate broader desires. Regardless, Russia uses a variety of methods of hybrid warfare to advance these goals, which can be categorized into three areas: activity that might be considered immoral or unethical by the United States and other nations but is not illegal (such as economic or political coercion), activity that occurs within the gaps and seams of international law and norms (such as cyber activity), or activity that is clearly in violation of international law or agreed norms but is not easily or clearly attributable to Russia as a state actor (such as intra- and extraterritorial assassinations). Given this intentional ambiguity surrounding Russia’s malign activity, deterring hybrid warfare is distinct from the context and logic of NATO’s conventional and strategic deterrence efforts during the Cold War.



Army Soldiers assigned to 1<sup>st</sup> Battalion, 319<sup>th</sup> Airborne Field Artillery Regiment, 3<sup>rd</sup> Brigade Combat Team, 82<sup>nd</sup> Airborne Division, operate M-777 Howitzer during live-fire exercise as part of Swift Response 21 at Tapa Central Training Area, Estonia, May 10, 2021 (U.S. Army/Michael Gressro)





## Deterrence in a Hybrid Warfare Context

Traditional Cold War deterrence used the capability/credibility/communication model within the context of mutually assured nuclear annihilation, and—despite academic debates about causality—it appears to have worked. Perhaps the most useful reframing of the problem is to consider hybrid warfare not as a single *thing* to be deterred. Rather, it is a *continuum* of activity synchronized to achieve a strategic objective, and it requires a collection of deterrence activity to reduce its likelihood and impact.

To deter Russia's use of hybrid warfare, the nation's operational approach must first be analyzed via component activities. Then, deterrence strategies that seek to impose costs and deny benefit should be created for each activity to limit Russian strategic flexibility and choice. While NATO can work within the Alliance to deny benefits for hybrid tactics, it lacks the ability to respond efficiently—or at all—as a unified front to impose costs by way of punishment. It is unlikely that a hybrid attack below the

level of armed conflict against a NATO member would be met with a unified NATO response. This is not necessarily a weakness, since NATO is not designed to engage in retributive attacks that do not meet the criteria for an Article V response.<sup>16</sup> However, as deterrence *credibility* hinges on a strong multilateral response, even if the response originated as a non-Alliance effort, it must appear to be a collective response within NATO's consensus-based decisionmaking process.

## Ways and Means to Deter Hybrid Warfare

**Comprehensive Defense.** If Russia employs all available means of national power in a hybrid warfare campaign, how could NATO equally mobilize resources to counter the threat? The first pillar to this answer is the concept of comprehensive defense. In comprehensive defense, policymakers designate their uniformed military forces as the focal point around which to organize a whole-of-society approach to national defense. This approach seeks to leverage the unique skills and capabilities of the military within joint military-civil

society initiatives that respond to complex security threats that no single institution acting alone could fully confront or effectively defeat. In this model, military forces drive unity of effort by organizing, training, motivating, and as appropriate, equipping the remaining population to achieve strategic objectives. By engaging the whole of their populations prior to a hybrid warfare campaign, NATO's Allies and partners could provide a multilayer defense to counter and preempt the full-court press of Russia's hybrid warfare strategy. Although defense and cost imposition occur on a continuum, the strategy can best be conceptualized using three distinct stages: baseline activities, competition below armed conflict, and armed conflict.

During baseline activities, comprehensive defense could be used to signal intent, build credible defense capability, and counter potentially hostile messaging campaigns against the population. Once organized into territorial defense units, auxiliary corps, neighborhood watches, concerned citizens groups, or any other number of structured organizations,

Operators from United Kingdom special forces sprint along catwalk following assault on oil rig during exercise Night Hawk 21 in Denmark, October 6, 2021 (NATO)



a nation's populace transforms from a potential target to a protective force. Instead of being ripe for exploitation by hybrid warfare tactics, a nation's population becomes a deterrence against them. Additionally, the act of organizing one's populace signals a nation's intent *not* to be a soft target for belligerent nations to manipulate. Once effectively transmitted, this signal alters the risk analysis of any country considering the use of hybrid warfare tactics. This is especially important in regions with ethnically Russian populations, such as Crimea or the Latgale region of Latvia, which are often the target of Russian hybrid activities. Organizing and uniting these populations with their states in advance places the initiative squarely on the friendly nation and denies many of the tactical advantages that Russian hybrid warfare relies on. Utilizing a whole-of-society approach amplifies the credibility of a nation's military defenses. A side benefit of organizing a country's population for comprehensive defense is that civilian organizations could also perform critical functions outside of countering hybrid warfare tactics. For example, maritime auxiliary units could perform

migration control-related tasks, and neighborhood watches could provide tips to fight organized crime or prevent acts of terrorism. Importantly, funding territorial defense units would allow a country to meet NATO defense spending targets while stimulating its own economy.

During competition below armed conflict, a nation's population could expose Russian actions, gather and pass intelligence, and counter Russian information operations (IO). A well-organized, informed, and motivated civilian population could be used to counter this aspect of hybrid warfare by denying an aggressor the ability to exert dominance in the information domain. Open-source and social media investigative organizations have already proved potent at countering Russian IO. Bellingcat, an independent collective of researchers and journalists, utilized simple, concrete investigative techniques to disprove numerous Russian disinformation campaigns, from their responsibility in the downing of Malaysian Airliner MH17 over Ukraine to poisonings by Russia throughout Europe.<sup>17</sup>

Bellingcat shows the power of the public to counter IO. Trained by their

military counterparts with similar capabilities (such as civil and public affairs or military intelligence and security forces), civilian organizations that understand the indicators of Russian hybrid warfare could identify and report malign activity—either to official government channels (becoming intelligence) or through the public domain (exposing the malign activity), informing populations in NATO and around the globe. This is especially important in areas with a large Russian diaspora or ethnic Russian population. The Alliance already recognizes that it faces Russian IO and combats the messaging in the Russian language.<sup>18</sup> Yet NATO need not assume sole responsibility to counter these threats. By organizing, educating, and training the population, a state could preempt and negate future Russian attempts to influence or take advantage of these vulnerable sectors. Additionally, both intelligence and information generated from organizing one's population are effective methods of imposing costs and limiting strategic options. Accurate and timely intelligence could support friendly nation counteractions while



broad exposure of malign activity helps build coalitions and sway public opinion. Timing is critical in this aspect of comprehensive defense—the earlier a population could accurately identify and report malign activity, the easier it would be for NATO’s members and partners to develop and implement a rapid response.

Finally, an organized and focused population could be used to supplement police forces, provide critical logistics and intelligence, and even augment friendly military forces during the transition from competition into armed conflict. The Russian hybrid warfare model has included a degree of armed (violent) conflict, although to a lesser intensity than the traditional fighting that would be a part of state-on-state armed conflict. For example, in eastern Ukraine, Russia’s hybrid warfare model quickly advanced from organizing demonstrations to the armed seizure of government buildings and military facilities.

During armed conflict, comprehensive defense could provide NATO members and partners with a large pool of resources. The concept of comprehensive defense also allows a nation to maintain this basic military capability at a much lower cost compared with maintaining a large active-duty force. History is replete with examples of nations rapidly expanding their military forces at the beginning of armed conflict—comprehensive defense provides the framework to do so and the deterrence against aggressors who seek to avoid this escalation.

Several aspects of comprehensive defense are already being implemented in the Baltic states. According to a 2019 RAND report, “total defense and unconventional warfare techniques and forces can support deterrence, early warning, de-escalation, [and] defense against invading forces.”<sup>19</sup> Estonia, Latvia, and Lithuania, as well as Poland, are increasing the capability of their territorial forces, national guards, and reserve forces and generating whole-of-society resilience and resistance efforts. These efforts to organize and engage the population are proving critical to counter Russian hybrid warfare efforts in the Baltics and should be used by all

threatened NATO members and partners as a template to combat Russian hybrid warfare. Individual members should seek to bolster comprehensive defense among Allies with every training event, exercise, or deployment available to NATO. Coordination with EU initiatives is a further mechanism to enable NATO members to pursue comprehensive defense. Initiatives such as the enhanced forward presence and tailored forward presence provide platforms for members to work together on comprehensive defense in addition to multinational conventional interoperability. U.S. joint force rotations are particularly capable of bolstering comprehensive defense through deterrence activities (such as the bomber task forces), intelligence support to the Alliance, deescalation, or if needed, defense with rotational presence.

*Information Operations.* Another critical aspect of imposing costs and limiting options available through Russia’s hybrid warfare approach is effective IO attribution and response. IO is substantive enough a factor in Russian hybrid warfare to be considered beyond comprehensive defense. Staying abreast of Russian hybrid objectives, methods, and tools prevents Allies and partners from being caught flat-footed. It also enables a better understanding of Russian intent and options for hybrid activity, both in traditional spheres and within the gaps and seams of 21<sup>st</sup>-century technology as an information platform. This analysis focuses on the intelligence- and information-gathering and strategic communication aspects of IO. Intelligence- and information-gathering are critical to identify Russia’s hybrid options and intent and to mobilize NATO member states toward the activity. Conversely, strategic communication is a proactive, comprehensive defense measure to specifically limit Russian hybrid options and to broadcast the costs Russia would incur if it moved forward with them.

For intelligence-gathering to be effective in today’s operating environment, countries must be willing to break down stovepipes and widely share information within their own government structures as well as with Allies and partners. The coordinated actions of hybrid warfare

allow Russia to exploit regional, national, and international seams. Building intelligence-sharing apparatuses both within and without ministries among and across countries helps to close those seams. Effective intelligence-sharing could occur at levels ranging from joint/multinational collection teams to finished intelligence analysis at ministerial or national levels. In other words, information-sharing does not always have to be top-down driven; sometimes bottom-up is effective.

One goal of shared intelligence is to reduce the time required for NATO to consult and respond in part or as a whole. This effort could be facilitated by a common intelligence picture shared by all parties. Partial, inconsistent, or stove-piped intelligence might slow NATO’s response process by creating doubt or failing to correctly attribute malign activity to the Russian government. In addition, whether internal to a state or between allied states, stovepiping challenges coordinated action against hybrid warfare. Better intelligence-sharing would allow states to deny Russia the benefit of using IO techniques in hybrid warfare to isolate specific states or populations. A common intelligence picture also makes it more likely, for example, that a Russian intelligence operative or team preparing to assassinate a dissident would be identified and detained, and have the network and messaging compromised. An example of intelligence-sharing success within NATO nations against hybrid activity is the Baltic Special Operations Forces Intelligence Fusion Cell, a budding Estonian, Latvian, Lithuanian, and Polish initiative that operates with assistance from the United States.<sup>20</sup> If implemented properly, such intelligence fusion cells might provide key indications and warnings of Russian hybrid warfare operations across the spectrum of IO, denying Russia the benefit of being able to claim noninvolvement/noninterference and could serve as a template for future initiatives among other Allies and partners. Furthermore, such fusion cells provide a path for connecting information across the Alliance’s multiple stovepipes, that is, the intra- and inter-bureaucratic inertia and the multilingual nature of the information environment. This enables



Army jumpmaster assigned to 1<sup>st</sup> Squadron, 91<sup>st</sup> Cavalry Regiment, 173<sup>rd</sup> Airborne Brigade, inspects paratroop door on C-130 Hercules before exiting paratroopers from III Infantry Brigade, Georgian Defence Force, during exercise Agile Spirit 21, Vaziani Training Area, Tbilisi, Georgia, August 1, 2021 (U.S. Army/John Yountz)

a common intelligence picture and, consequently, the ability of the Allies to collectively deny Russian IO to access seams unfettered and without attribution.

Once Russian hybrid warfare IO activity is recognized and NATO agrees a response is appropriate, strategic communication would likely be employed as the principal countermeasure and vanguard to prevent Russian activity. The situational awareness derived from the shared information and intelligence discussed in the previous section would be critical to crafting targeted messages. Strategic communication would likely be split between two audiences: external actors and an audience internal to the conflict (that is, the targeted population). Internal strategic communication efforts should focus on countering the information aspect of hybrid warfare. Prior to a campaign, successful strategic communication might

limit the vulnerability to target audiences, such as the Russian-speaking minorities of the Baltic states, or a Russian hybrid campaign. This is achieved by negating Russia's plausible deniability concerning the sponsorship of the conflict's version of "little green men" (or whatever the aggressor looks like in that campaign). Internal strategic messaging campaigns must be swiftly organized and executed because they are most effective if they prevent Russia from gaining a tactical advantage during the initial "fog of war" period. Once a hybrid warfare campaign has begun, the focus of external strategic communication should be to expose Russian activities to NATO (and the rest of the world). This might undermine Russian public support for such activities, would inform decisionmakers during NATO deliberations, and should unite the international community against the malign actor.

*Ally and Partner Contribution and Collaboration.* Comprehensive defense enables unity of effort across militaries, governmental institutions, and societies within the Alliance. This unity of effort requires a strategic evolution within NATO, particularly in understanding and combating nonstandard aggression outside the traditional attacks or threats captured within Article IV and Article V of the Washington Treaty.<sup>21</sup> NATO member states and partners have tremendous capacity beyond their armed forces to deter Russian hybrid warfare activity and impose costs. Experience and specialization among NATO's members allow for nuanced strategic planning to anticipate and respond to the use of hybrid warfare and enable distinct capacities to be employed to impose costs. NATO leadership could harmonize efforts and ensure that resistance measures synthesize among member states.

Simplifying hybrid warfare deterrence means analyzing synchronized Russian activities and countering them separately. To this end, individual member states might utilize and reinforce their civil and military strengths to combat discrete hybrid activities. NATO should complement these efforts and enable specialization and interconnectedness among Allies. In the traditional military model, NATO desires uniformity and interoperability. Against hybrid activities, individual member states' niche capabilities and strengths are assets. For example, after the unprecedented 2007 Russian cyber attack on Estonia targeting non-military infrastructure via nonstandard means, Estonia revolutionized its cyber capability and capacity in both military and civilian infrastructure and expertise.<sup>22</sup> Estonia's encryption and defense of its electronic systems led in generating civil-government cooperation, and Estonia understands how Russian cyber activity regularly targets its information technology networks. This development helps to deter Russian attacks. Furthermore, the ability to attribute such activity by an Ally helps the collective Alliance impose costs, which, as former Estonian President Toomas Hendrik Ilves demonstrated, need not be responded to in-kind in the cyber environment.<sup>23</sup> Alliance members could respond with other instruments of power (for example, diplomatic or economic) as the result of individual member strengths. This proficiency demonstrates how one Ally could contribute to the security of all. As a regional leader in cyber security, Estonia now serves as a capacity and capability vanguard for the other Allies, from whom Allies should learn and grow. For example, U.S. Cyber Command recently collaborated with its Estonian counterparts to strengthen both nations' cyber defenses.<sup>24</sup>

Indeed, while NATO is perceived to be at a disadvantage because it comprises 30 states with 30 different national priorities, strategies, interests, and militaries, NATO's diversity could also be a source of strength. Allies could spearhead initiatives based on their strengths and share the boon of their efforts. There is significant capacity among Allies to build

resistance networks that would impose costs. Poland and the three Baltic states are among those NATO members that have militias or civil institutions organized to combat occupation. These forces could also partner with other elements, such as border guards and police forces, to ensure that a nonstandard attack or provocation is prevented or subverted to deny hybrid warfare options to Russia and encourage restraint.

Other partners have experience with Russian hybrid warfare threats, often at a level much higher than other NATO nations. NATO could learn tremendously through the expansion of cooperation with Georgia and Ukraine, both of which have suffered for years from Russia's hybrid activity. Both nations have adapted to multiple issues—occupied terrain, denied access to populations, and competition over media narratives and legitimacy, as well as a constant pressure on their political, civil, and social institutions.

Ukrainian and Georgian partnership with NATO members is strong. Multiple initiatives exist to help modernize and professionalize the Ukrainian military. One notable example is the Comprehensive Assistance Package, which NATO members pledged to in the Warsaw 2016 Summit, and which explicitly identified hybrid warfare among its topic areas.<sup>25</sup> These initiatives guide NATO support to Ukraine and enable dialogue, including a joint platform on hybrid warfare last held in November 2018.<sup>26</sup> This platform should continue, as such collaborations could harden both Ukraine and the Alliance to hybrid warfare. Likewise, similar platforms should be built on and expanded to target Russia's calculus and prevent hybrid warfare against critical partners.

While Russian hybrid efforts stalled Georgia's 2008 Membership Action Plan into NATO, it has not halted continued partnership and collaboration.<sup>27</sup> The 2016 Substantive NATO-Georgia Package, a broad set of initiatives designed to modernize Georgia's military and achieve NATO interoperability because of the Wales Summit, oddly omits discussion of hybrid warfare.<sup>28</sup> This presents an opportunity for NATO to develop

hybrid warfare platforms (like those with Ukraine) to collaborate with Georgia on. Through partnerships and collaborations such as these, NATO could learn from previous experiences and be better prepared to prevent future hybrid threats.

## Conclusion

As Russia has evolved to increasingly rely on hybrid warfare as a major component of its strategy, NATO must adapt accordingly. NATO's model must shift from a reliance on traditional military deterrence and expand to incorporate political, economic, and social spheres to counter aggression below the level of armed conflict. Since NATO's structure does not readily support innovation or active (versus passive) deterrence measures, new ideas and emphases are needed to address these challenges.

Pursuing activities to deter hybrid warfare certainly poses risks and challenges to NATO and its member states and partners. Activities in these spheres might risk further blurring lines between military and nonmilitary responsibilities. Individual member laws and EU regulations might complicate these efforts. Civil institutions could be at risk of being identified as military targets in the event of a linear war.

Consequently, Allies and partners must update their methods to better deter Russian aggression by reducing Russia's strategic options and increasing their own ability to impose costs. Imposition of costs via Allies' domains of diplomatic, information, military, and economic levers are central to changing Russia's cost-benefit assessment regarding hybrid warfare and enabling deterrence. Doing this could be achieved through such concepts as comprehensive defense, improved IO, and expanded allied member and partner collaboration. While the overall goal of maintaining Alliance unity and solidarity remains the same, the means and ways through which Allies and partners achieve that goal should change. This includes embracing the diversity of members' strengths and capabilities and exploring increased partnerships with non-NATO members to leverage and

learn from their experience with Russian hybrid warfare aggression.

The primary limitation of this analysis is the inability to prove the effectiveness of this proposal in deterring future Russian hybrid warfare. As deterrence prevents action, how does one measure inaction? How could one attribute causation? To this end, the lessons of nuclear deterrence during the Cold War might hold some answers. Further examination of academic literature and public policy best practices could help to identify and develop measures of deterrence effectiveness. Once this framework or methodology is established, the hypotheses and proposals laid out in this article could be tested like those at the height of the Cold War. JFQ

## Notes

<sup>1</sup> James K. Wither, “Making Sense of Hybrid Warfare,” *Connections* 15, no. 2 (2016), 73–87.

<sup>2</sup> *Hybrid Warfare*, GAO-10-1036R (Washington, DC: U.S. Government Accountability Office [GAO], September 10, 2010), 1–19, available at <<https://www.gao.gov/products/gao-10-1036r>>.

<sup>3</sup> Wither, “Making Sense of Hybrid Warfare,” 79–81. Note that Russian terminology includes the terms *new generation warfare* as well as *nonlinear war*.

<sup>4</sup> The European Centre of Excellence for Countering Hybrid Threats, “Hybrid Threats,” available at <<https://www.hybridcoe.fi/hybrid-threats/>>.

<sup>5</sup> Kestutis Paulauskas, “On Deterrence,” *NATO Review*, August 5, 2016, available at <<https://www.nato.int/docu/review/articles/2016/08/05/on-deterrence/index.html>>.

<sup>6</sup> North Atlantic Treaty Organization (NATO), “London Declaration,” press release, December 4, 2019, available at <[https://www.nato.int/cps/en/natohq/official\\_texts\\_171584.htm](https://www.nato.int/cps/en/natohq/official_texts_171584.htm)>.

<sup>7</sup> Ibid.

<sup>8</sup> John F. Kennedy, “The President and the Press: Address Before the American Newspaper Publishers Association, April 27, 1961,” Waldorf Astoria Hotel, New York City, John F. Kennedy Presidential Library and Museum, available at <<https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-newspaper-publishers-association-19610427>>.

<sup>9</sup> Christopher S. Chivvis, *Understanding Russian “Hybrid Warfare” and What Can Be*

*Done About It*, Testimony Before the House Armed Services Committee, 115<sup>th</sup> Cong., 1<sup>st</sup> sess., March 22, 2017, available at <[https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND\\_CT468.pdf](https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf)>.

<sup>10</sup> “Estonia Fines Man for ‘Cyber War,’” BBC News, January 25, 2008, available at <<http://news.bbc.co.uk/2/hi/technology/7208511.stm>>.

<sup>11</sup> European Union, *Independent International Fact-Finding Mission on the Conflict in Georgia*, vol. 1 (September 2009), 18–22, available at <[https://www.echr.coe.int/Documents/HUDOC\\_38263\\_08\\_Annexes\\_ENG.pdf](https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf)>.

<sup>12</sup> For recent reference, see United Nations, “Resolutions Calling on Withdrawal of Forces from Crimea, Establishing Epidemic Preparedness International Day Among Texts Adopted by General Assembly,” press release, December 7, 2020, available at <<https://www.un.org/press/en/2020/ga12295.doc.htm>>.

<sup>13</sup> Fiona Hill, “This Is What Putin Really Wants,” Brookings, February 24, 2015, available at <<https://www.brookings.edu/opinions/this-is-what-putin-really-wants/>>; Julia Ioffe, “What Putin Really Wants,” *The Atlantic*, January/February 2018, available at <<https://www.theatlantic.com/magazine/archive/2018/01/putins-game/546548/>>.

<sup>14</sup> Uğur Celil Özgöker and Serdar Yilmaz, “NATO and Russia’s Security Dilemma Within the European Union’s Far Neighbors,” *International Relations and Diplomacy* 4, no. 10 (October 2016), 650–665.

<sup>15</sup> Bettina Renz and Hanna Smith, *Russia and Hybrid Warfare—Going Beyond the Label*, Aleksanteri Papers (Helsinki, Finland: Kikimora Publications at the Aleksanteri Institute, University of Helsinki, January 2016), available at <[https://helda.helsinki.fi/bitstream/handle/10138/175291/renz\\_smith\\_russia\\_and\\_hybrid\\_warfare.pdf](https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf)>.

<sup>16</sup> Article V of the Washington Treaty clarifies and affirms NATO members to collective defense in the event of an attack. See NATO, “The North Atlantic Treaty,” updated April 10, 2019, available at <[https://www.nato.int/cps/en/natolive/official\\_texts\\_17120.htm](https://www.nato.int/cps/en/natolive/official_texts_17120.htm)>.

<sup>17</sup> Bellingcat, “About,” available at <<https://www.bellingcat.com/about>>.

<sup>18</sup> NATO, “NATO’s Approach to Countering Disinformation: A Focus on COVID-19,” updated July 17, 2020, available at <<https://www.nato.int/cps/en/natohq/177273.htm>>.

<sup>19</sup> The concepts of *total defense* and *unconventional warfare* are like the concept of *comprehensive defense*. The authors define *total defense* as “a whole-of-society approach to national defense and resilience . . . and broad-based, state-supported resistance against invaders . . . designed to enhance deterrence by denial and by increasing the cost of

aggression.” This mutually supporting idea provides an example of how comprehensive defense is naturally evolving in the Baltics in response to potential Russian aggression. See Stephen J. Flanagan et al., *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance* (Santa Monica, CA: RAND, 2019), 1, available at <[https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR2700/RR2779/RAND\\_RR2779.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2779/RAND_RR2779.pdf)>.

<sup>20</sup> “How the Baltic States Spot the Kremlin’s Agents,” *The Economist*, August 1, 2019, available at <<https://www.economist.com/europe/2019/08/01/how-the-baltic-states-spot-the-kremlins-agents>>.

<sup>21</sup> Article IV of the Washington Treaty enables consultations among the Allies whenever the “territorial integrity, political independence or security” of any member is threatened. Article V clarifies and affirms the members to collective defense in the event of an attack. See NATO, “The North Atlantic Treaty.”

<sup>22</sup> Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 69–72.

<sup>23</sup> Toomas Hendrik Ilves, “The Consequences of Cyber Attacks,” *Journal of International Affairs* 70, no. 1 (2016), 175–181.

<sup>24</sup> U.S. Cyber Command, “Hunt Forward Estonia: Estonia, U.S. Strengthen Partnership in Cyber Domain with Joint Operation,” December 3, 2020, available at <<https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/>>.

<sup>25</sup> NATO, “Relations with Ukraine,” updated January 11, 2020, available at <[https://www.nato.int/cps/en/natolive/topics\\_37750.htm](https://www.nato.int/cps/en/natolive/topics_37750.htm)>.

<sup>26</sup> *NATO’s Support to Ukraine*, NATO factsheet (Brussels: NATO, November 2018), available at <[https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2018\\_11/20181106\\_1811-factsheet-nato-ukraine-sup.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181106_1811-factsheet-nato-ukraine-sup.pdf)>.

<sup>27</sup> Daniel Dombey, “U.S. Gives Way on NATO for Georgia and Ukraine,” *Financial Times*, November 26, 2008, available at <<https://www.ft.com/content/b48201e0-bc00-11dd-80e9-0000779fd18c>>; NATO, “Relations with Georgia,” updated August 25, 2021, available at <[https://www.nato.int/cps/en/natohq/topics\\_38988.htm](https://www.nato.int/cps/en/natohq/topics_38988.htm)>.

<sup>28</sup> *Substantial NATO-Georgia Package (SNGP)*, NATO factsheet (Brussels: NATO, 2017), available at <[https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2017\\_02/20170221\\_1702-georgia-sngp-factsheet-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170221_1702-georgia-sngp-factsheet-en.pdf)>.

*Capture of Monterey [sic], on September 21–24, 1846, during Mexican-American War, at Monterrey, Nuevo León, Mexico; lithograph by Adolphe Jean-Baptiste Bayot, after drawing by Carl Nebel, 1851 (George Kendall and Carl Nebel)*



# Improvised Partnerships

## U.S. Joint Operations in the Mexican-American War

By Nathan A. Jennings

From 1846 to 1848, the United States and Mexico fought a controversial war to decide which of the great republics would be the dominant power in North America. Featuring a series of U.S. invasions that spanned from San Diego to Veracruz, the 26-month contest included bloody

set-piece battles between national armies, aggressive maritime blockades and amphibious assaults along the Pacific and Atlantic coasts, and prolonged occupations that invited a savage guerrilla resistance. As historian K. Jack Bauer stated in his foundational study, *The Mexican War*, the conflict was “fought with doggedness by the soldiers and sailors of both nations under the leadership of brilliant and inept commanders,” as political leaders struggled over differing ideas of a “reasonable political settlement.”<sup>1</sup>

The histories of the resulting American victory have largely credited a combination of U.S. Army battlefield superiority and Mexican internal disunity for the outcome. However, while decisive victories at Palo Alto, Buena Vista, Cerro Gordo, and Mexico City proved critical, deeper analysis reveals that it was rather a pragmatic willingness to form ad hoc partnerships between the U.S. Army and the U.S. Navy—and to a lesser extent, the U.S. Marine Corps and the precursor to the U.S. Coast Guard, the Revenue Cutter Service—that provided the

---

Major Nathan A. Jennings, USA, Ph.D., is an Army Strategist and Assistant Professor in the Department of Military History at the U.S. Army Command and General Staff College.



necessary capabilities to win and endure in enemy territory.<sup>2</sup> Viewed in modern doctrinal terms, the U.S. military's land and maritime forces won in Mexico by engaging in "team warfare," which expanded and extended a continental scope of strategic pressure that ultimately allowed the achievement of national objectives.<sup>3</sup>

Despite the lopsided outcome of the war, the American armies and fleets that relied on each other to invade Mexico began the conflict unprepared to devise and execute a joint expeditionary concept. The small U.S. military establishment at that time had yet to establish codified joint doctrine, and its mostly dismal performances during the War of 1812 in the Great Lakes region and along the Atlantic seaboard left the growing nation without a working precedent for large-scale cooperation among Services. This deficit consequently required individual commanders to negotiate command relationships and operational priorities in deployed settings, which predictably resulted in friction between outside personalities and conflicting agendas.<sup>4</sup>

Yet, while the absence of a preexisting joint framework created challenges, the U.S. military's ability to improvise partnerships ultimately enabled the achievement of most strategic aims. The American officers' unprecedented success at forming ad hoc teams in Mexico—though strained under the weight of professional and cultural biases—allowed U.S. Army, Marine Corps, Navy, and Revenue Cutter Service contingents to project and sustain the necessary land-power required to, as euphemistically stated by the Army's commanding general, Winfield Scott, "conquer a peace."<sup>5</sup> This pragmatic approach to integrating diverse capabilities established a nascent precedent for an emerging American way of war—one that now embraces joint expeditionary cooperation as a cornerstone of its 21<sup>st</sup>-century character.

## Strategic Background

The outbreak of general war between the United States and Mexico in April 1846 found both republics unprepared for a continental conflict. Though the Americans boasted a larger population

and industry, they began the war with a Regular Army of just 7,365 men conducting mostly frontier and garrison duties. This focus ensured that its dispersed companies and regiments lacked practical experience in conducting consolidated, large-scale maneuvers. In the maritime domain, the U.S. Navy divided a modest complement of steam-powered frigates among its Home Squadron, West Indies Squadron, and Africa Squadron. The U.S. Marine Corps and Revenue Cutter Service completed the military establishment by providing limited maritime assault and shallow-water support.<sup>6</sup>

Mexico likewise possessed a dispersed military establishment that stood ill-prepared to concentrate for big campaigns. After decades of fractious politics and internal rebellion, the Mexican government fielded an army of almost 19,000 men—with potential to double its size via conscription. However, though larger than its *Norte Americano* counterpart and led by an experienced officer corps, the Mexican army fought with outdated weaponry and used outdated logistical practices.<sup>7</sup> The small Mexican navy—consisting of 14 vessels with the Department of the North in the Gulf of Mexico and another 2 vessels with the Department of the South in the Pacific—likewise sailed unprepared to contest control of the maritime domain with just 2 steam-powered ships.<sup>8</sup>

Regardless of wartime readiness, the U.S. annexation of Texas—and more important, inherited claims of territory along the north bank of the Rio Grande—swiftly drew the two republics into armed conflict. While the expansionist-minded James K. Polk administration emphasized the Texas claim, its real strategic aim centered on acquiring California and its deep-water ports that would enable commerce with the Far East. Mexico, for its part, refused to sell the valuable territories out of nationalistic pride and dispatched its Army of the North to defend Mexican interests. The movement of a small American force under future President Zachary Taylor to the north bank of the Rio Grande in March 1846 made a clash of arms

inevitable as the continental powers postured to decide the issue.<sup>9</sup>

The sudden onset of war would challenge both the American and Mexican military establishments with requirements to mobilize and fight in distant expeditionary settings. In Washington, DC, even as Taylor engaged the Mexican army on the Texas frontier, President Polk devised a strategy to seize initiative—by launching two incursions along the Rio Grande frontier with a third force attacking through New Mexico to capture California. Simultaneously, the U.S. Navy neutralized the Mexican navy, blockaded major ports in the Gulf of Mexico, and seized coastal towns in California. On the other side, to compel a favorable settlement, Mexico aimed to attain an early offensive victory over Taylor while defending its frontier provinces. For both sides the challenges of projecting force in multiple domains stressed preconceived notions about 19<sup>th</sup>-century warfare.

## Initial Expeditions, 1846

The opening salvos of the Mexican-American War occurred north of the Rio Grande when, following a cavalry skirmish that gave Polk a questionable *casus belli*, Taylor's force of 3,554 men defeated Mexico's Army of the North on May 8 and 9 in the twin battles of Palo Alto and Resaca de la Palma. The expedition's use of innovative "flying artillery" to disrupt the Mexican infantry proved particularly instrumental in securing the victory. The Americans then crossed the river, marched on the provincial capital of Monterrey, and took the imposing fortress by storm. With the Mexicans in disarray and retreat, many considered the war almost over, as Taylor's regiments dispersed to occupy and control the region until a treaty agreement could be arranged.<sup>10</sup>

Simultaneous to the U.S. Army's engagements in the Rio Grande theater, the U.S. Navy commenced an aggressive campaign in the Gulf of Mexico to neutralize the smaller enemy fleet and blockade all major ports. Although attaining maritime dominance proved relatively easy, the decision to occupy major ports proved more difficult due

to Mexico's land defenses and shallow-water approaches. This aspect of the U.S. Navy's campaign intensified with significant amphibious assaults by U.S. Marines on the major port towns of Tabasco and Tampico; the goal was to isolate northeastern Mexico and support Taylor's inland operations. The possession of Tampico, specifically, would prove useful the next year as an intermediate staging base to facilitate a larger offensive against the fortified port city of Veracruz to the south.

If the U.S. Navy proved its value by establishing Mahanian fleet dominance, the much smaller Revenue Cutter Service proved initially valuable in providing river-borne support to the U.S. Army as it marched into the Mexican interior. This aid included transporting troops, weapons, and supplies up the Rio Grande; carrying dispatches back to the United States; and patrolling against opportunistic Mexican privateers. While possessing smaller cannons than their naval counterparts, the Revenue Cutters proved useful in penetrating shallow waterways that precluded heavier vessels, and these Servicemen earned rare praise from the Home Squadron commander for facilitating the capture of Alvarado and Tabasco.<sup>11</sup>

Simultaneous to the joint operations unfolding in the Gulf of Mexico, the U.S. West Indies Squadron, also called the Pacific Squadron, commenced a significant naval effort to wrest Alto California from Mexican control. After positioning along the coast to await a declaration of war from Washington, DC, Commodore John Sloat occupied the provincial capital of Monterrey on July 7 and seized the future town of San Francisco. When a new commodore, Robert Stockton, assumed command, he sent a force of U.S. Marines and Sailors to occupy Los Angeles; however, a counterattack by *Californios* under Governor José María Flores retook the city and instigated a tumultuous series of reversals as American and Mexican forces fought for control of the coastal province.<sup>12</sup>

While the U.S. Navy initiated operations in California, the U.S. Army's 1<sup>st</sup> Regiment of Dragoons, under General

Stephen W. Kearny, arrived to assist in the capture of the coveted province following a debilitating 1,000-mile ride from Fort Leavenworth, Kansas. However, a force of Mexican Lancers under Major Andrés Pico intercepted and defeated the dragoons at the Battle of San Pasqual, east of San Diego, and compelled them to seek desperate help from Stockton on the coast. This setback, which followed a previous defeat of the naval contingent at the Battle of Dominouez Rancho by Flores's resurgent *Californios* 2 months prior, placed the scattered American expedition in jeopardy, as it appeared that Mexico would preserve its control of the region.<sup>13</sup>

On December 12, 1846, Stockton and Kearny regrouped in San Diego and planned a joint approach that aimed to mass combat power to finally defeat the Mexican defenders. Incorporating Captain John C. Fremont's California Battalion, which consisted of Anglo settlers who had revolted against Mexican rule, the four contingents—Soldiers, Marines, Sailors, and militia—united to form an ad hoc regiment of 550 men to march on Los Angeles. The American force, which both Stockton and Kearny claimed to command, then defeated Flores's *Californios* at the Battle of Río San Gabriel on January 8, 1847, and routed the Mexicans at the Battle of La Mesa the next day. The victors' subsequent march into Los Angeles definitively settled ownership of California in favor of the United States.<sup>14</sup>

Although Stockton and Kearny had managed to unite and defeat the *Californios*, the two men immediately launched into a caustic quarrel over who would command the conquered territory. In the absence of joint doctrine or hierarchies, both commanders claimed that their respective military departments had ordered them to assume command. The situation became further complicated when Stockton tried to establish Fremont as governor and Kearny retreated to San Diego to await U.S. Army reinforcements. The problem was resolved only when General Scott sent specific orders for the Army to assume control of the civil government, with the Navy in charge

of port affairs only. When Fremont refused to enlist his settlers under U.S. Army control, Kearny arrested him and brought him back to Fort Leavenworth for court martial.<sup>15</sup>

This success in the West, though marred by discoordination and rivalry, left the U.S. Army with a vast chain of garrisons from San Diego to Matamoros; the U.S. Navy controlled both the California and Gulf of Mexico coastlines. However, in February 1847, President Antonio López de Santa Anna led 15,000 men north to seize initiative by attacking Taylor in perhaps the most important engagement of the war: the Battle of Buena Vista. With most of the U.S. Army Regulars diverted in preparation for a littoral invasion of central Mexico, Taylor's remaining volunteer regiments fought a difficult, defensive fight that managed to turn back the Mexicans while inflicting more than 3,000 casualties.<sup>16</sup> This costly victory preserved American control of northern Mexico and initiated a new and desperate phase of the war.

### **Increasing Strategic Pressure, 1847–1848**

The year 1847 began with the Polk administration demanding that Mexico sell the northern territories then under U.S. occupation and the Mexican government refusing to comply. Considering the "political instability" and "obstinacy of the enemy," Scott, then supervising the war from Washington, DC, proposed to "open a new and better line of operation upon the enemy's capital."<sup>17</sup> Seeking to increase political pressure, he planned to seize the port fortress of Veracruz along the Gulf coast, march inland toward Mexico City, defeat any remaining Mexican armies, and finally compel the government to agree to terms. This expedition required the largest joint amphibious operation in American history to date, while offering high risk and reward for the invading forces.

The Mexico City campaign unfolded from the outset as a massive and complicated joint venture. With the bulk of the Regular Army regiments requiring shipment from the Rio Grande theater, the U.S. Army concentrated more than



*War News from Mexico* by Richard Caton Woodville, Sr., oil on canvas, 1848 (Crystal Bridges Museum of American Art, Bentonville, Arkansas)

200 ships consisting of escort frigates, transport vessels, supply ships, cutters, and specially designed landing craft to transport Scott's 11,000 men for an amphibious assault on Veracruz. Called the "Gibraltar of the West" due to its

impressive fortifications, the fortress city posed an enormous challenge to those seeking access to the Valley of Mexico. Nevertheless, by March 7 the U.S. Navy had transported the entire ground force to the point of final debarkation along

the littoral coast and reinforced its blockade of Veracruz's impregnable island castle, San Juan de Ulúa.<sup>18</sup>

Early on March 8, under the supervision of Commodore David Connor, the Navy employed 67 surfboats to





U.S. Army, commanded by General Zachary Taylor, near Corpus Christi, Texas (from the north), October 1845, during Mexican-American War; lithograph by Charles Parsons, after drawing by Daniel Powers Whiting (Library of Congress)



General Winfield Scott enters Mexico's capital during Mexican-American War in 1847, in "American Army Entering the City of Mexico," as part of *The Frieze of American History*, in U.S. Capitol Rotunda, by Constantino Brumidi, Filippo Costaggini, and Allyn Cox (Architect of the Capitol)

successfully land the assault forces south of Veracruz. In under 5 hours, the Sailors delivered 8,600 Soldiers and Marines to the target beaches—a remarkable feat given the unprecedented nature of the operation for the U.S. military. With the U.S. Navy blockading the fortress, Scott proceeded to encircle and bombard the city's 3,300 defenders and 15,000 civilians with a line of field cannons and mortars—all while deflecting several relief attempts by external Mexican forces. The Navy then offloaded six 32-pound cannons with gun crews from its ships to intensify the assault. After enduring 4 days of unrelenting destruction and casualties, the Mexican garrison finally surrendered.<sup>19</sup>

With theater access assured, Scott proceeded to march west to Mexico City with the intent to compel favorable negotiations. While the U.S. Navy protected sea lines of communication back to the United States, the U.S. Army won another decisive victory on April 18, 1847, when it shattered Santa Anna's final field army at Cerro Gordo. Scott then occupied the town of Puebla to establish an intermediate base, temporarily severed his supply lines stretching back to Veracruz, and continued west to Mexico City. The campaign culminated with a series of American assaults on the fortified Mexican capital, which resulted in its government fleeing into exile and the invaders establishing a tenuous occupation of the Valley of Mexico and its 2.3 million inhabitants.<sup>20</sup>

Throughout the advance on Mexico City, a Marine Corps battalion under command of Lieutenant Colonel Samuel Watson supported the march. Arriving in Veracruz in July, the Marines joined a reinforcement column of U.S. Army volunteers and moved west to participate in the capture of Mexico City. Throughout the long march, Watson's men fought off guerrilla attackers (a rising problem for the spreading American lines of communication) and eventually joined the main force to take a leading role in the assault on the Chapultepec Castle. The Marines then battled their way into the capital, earning high praise for being among the first Americans to enter the city and occupy the "Halls of Montezuma." Watson, who had earned distinction for bravery, succumbed to illness shortly afterward and died in Veracruz.<sup>21</sup>

By mid-September 1847, the U.S. military had established dominance over Mexico on land and at sea. Yet the Mexican government, now in exile, still refused to concede defeat. It instead embraced a decentralized guerrilla campaign designed to "attack and destroy the Yankees' invading army in every way imaginable" in a "war without pity."<sup>22</sup> Prioritizing swift cavalry tactics, the Mexican guerrillas assaulted both Scott's and Taylor's lines of communication in an attempt to isolate occupying garrisons. When both generals responded by recruiting mounted Texas Ranger regiments to counter the elusive resistance, the war became a bitter contest

over which side could outwait the other's political tolerance for the costs of large-scale occupation and the atrocities that inevitably occurred.<sup>23</sup>

Throughout 1847, as the U.S. Army maintained a fragile hold on the Mexican interior, the U.S. Navy, Marine Corps, and Revenue Cutter Service performed a vital role in both sustaining the sprawling land occupation and expanding maritime pressure along the Pacific and Atlantic coasts. The Home Squadron, now under command of Commodore Matthew Perry, seized the Gulf towns of Alvarado and Tuxpan in April and then formed a 1,173-strong "Naval Brigade" to finally capture the holdout port of Tabasco in June. As before, Revenue Cutters provided valuable shallow-water capability for upriver naval expeditions while Marine detachments, with Sailor augmentation, supplied assault capability to oust the remaining Mexican garrisons.<sup>24</sup>

To the west, the Pacific Squadron likewise pressed forward to increase maritime pressure on the beleaguered Mexican government. This campaign unfolded as a series of blockades and offensives against Mazatlán, Mexico's largest Pacific port, and sporadic attempts to neutralize military garrisons along Baja California. Employing the newly arrived 1<sup>st</sup> Regiment of New York Volunteers as reinforcements, the squadron seized, and sometimes lost, control over coastal cities such as San José del Cabo, La Paz, Guaymas, San Blas, and Todos Santos. Although the

blockade suffered from logistical issues and Mexican counterattacks, the campaign succeeded in creating additional dilemmas for the Mexican national leadership and, more important, protected American gains in Alto California.<sup>25</sup>

The combined efforts of the U.S. military across Mexico, reflecting the first large-scale joint operations in American history, finally compelled the Mexican government to sign the Treaty of Guadalupe Hidalgo on February 2, 1848. With their northern provinces, capital region, and major ports under seemingly permanent occupation, and other regions such as Zacualtipán and the Yucatan now rising in rebellion, the Mexican leadership ceded rights to Texas and sold its vast northern provinces to the United States for a price of \$15 million—less than half the amount Polk had offered prior to the war. In a historical irony, the U.S. military's final action in Mexico was to reconstitute and rearm the broken Mexican army so that

Mexico City could restore stability and enforce the new borders.<sup>26</sup>

### Insights for Joint Warfare

The U.S. military's decisive victory in the Mexican-American War stemmed, in part, from a forward-thinking approach to conducting joint operations across an expansive and multitheater contest. Throughout the controversial conflict, the U.S. Army, Marine Corps, Navy, and Revenue Cutter Service joined mostly complementary, though sometimes counterproductive, efforts across land and maritime domains to project and sustain expeditions of a continental scale. As now mandated in Joint Publication 3-0, *Joint Operations*, American military forces in that era—in the absence of codified joint doctrine and prior joint experience—improvised partnerships to leverage the “synergy” created by “the integration and synchronization of military operations in time, space, and purpose.”<sup>27</sup>

This convergence of land and maritime efforts proved critical in allowing the United States not only to win a sequence of decisive set-piece battles against the larger Mexican army but also to sustain the broader war effort long enough to compel the Mexican government to concede defeat. Without the U.S. Navy's ability to neutralize the Mexican fleet, secure sea lines of communication, provide combat power to land engagements, and expand the blockade along both oceanic coasts, the U.S. Army would have faced significant—and potentially debilitating—challenges in translating battlefield victories into enduring gains. The resulting capacity to extend and expand landpower into early 1848 ultimately empowered the Polk administration's negotiation position and led to the achievement of policy aims.

This increase in fighting capacity benefited from a significant wartime expansion of the relatively small U.S. military establishment to meet operational



“Landing of the American Forces under General Scott, at Vera Cruz, March 9, 1847,” Currier & Ives (Library of Congress)

requirements. While the U.S. Army grew from an authorized strength of 8,613 Soldiers to 30,954 Regulars and 73,776 volunteers, the Marine Corps increased from 1,263 men scattered across ship-based detachments to create a full-size infantry regiment to fight in the land campaigns.<sup>28</sup> The U.S. Navy, now authorized to increase to 11,000 Sailors, added personnel to man its dramatically expanded fleet, which resulted from both newly constructed ships and captured Mexican vessels. This rapid wartime growth, which also required a heavy reliance on civilian contract support in the form of merchants and teamsters, made a more robust joint concept possible and allowed an increase in American ability to mass forces and maintain operational endurance.

Another insight from this war centers on the importance of unity of command and shared vision. In the turbulent California Campaign, leaders from different Services arrived with uncoordinated operational approaches and lacked an agreed-upon plan for an efficient transition to postconflict governance. This absence led Stockton and Kearny to suffer initial defeats in detail after failing to synchronize their converging maritime and land offensives. When they recovered and finally defeated the Californios with a joint offensive, the egotistical commanders fell into acrimonious disputes over who would lead the consolidation of gains. Bitter disagreements over control of militia then further undermined unity of command and threatened to destabilize the new U.S. territory.

If the California effort stands as a cautionary lesson, the much larger expedition to seize Veracruz the next year remains a model for jointness. In that campaign, Scott's central idea to create "further brilliant victories on a single line of operations toward the capital," while "aided by the blockading squadron off the coast," established a clear, unified operational approach.<sup>29</sup> Throughout the operation, the involved Army and Navy leadership recognized Scott's seniority, conducted collaborative planning prior to execution, reinforced the landing parties with naval firepower, and transitioned to agreed-upon roles following the city's surrender.

This successful "integration" of "joint functions," as described by modern U.S. doctrine, established conditions for a successful march on Mexico City.<sup>30</sup>

In the final analysis, the performance of the U.S. military in the Mexican-American War instituted a fundamental and enduring precedent for the modern American way of war. The unified efforts of the U.S. Army, Marine Corps, Navy, and Revenue Cutter Service from 1846 to 1848 established inter-Service cooperation as a cornerstone of future U.S. expeditionary campaigns. In historic terms, the victory catapulted the United States into the position of dominant power in North America and set conditions for global expansion in the 20<sup>th</sup> century. Though still controversial in origin and outcome, the U.S. military's performance in Mexico—across both the land and maritime domains and despite unprecedented requirements for joint cooperation—remains an important achievement in the history of American arms. JFQ

## Notes

<sup>1</sup> K. Jack Bauer, *The Mexican War, 1846–1848* (Lincoln: University of Nebraska Press, 1992), 399.

<sup>2</sup> See Richard Bruce Winders, *Mr. Polk's Army: the American Military Experience in the Mexican War* (College Station: Texas A&M University Press, 1997); K. Jack Bauer, *Surfboats and Horse Marines: U.S. Naval Operations in the Mexican War, 1846–48* (Annapolis: United States Naval Institute, 1969); Gabrielle M. Neufeld Santelli, *Marines in the Mexican War*, Occasional Paper Series, ed. Charles R. Smith (Washington, DC: Headquarters U.S. Marine Corps, 1991); and Robert Jay Lloyd, "Serving in Obscurity: Operations in the Gulf of Mexico During the Mexican American War, 1846–1847" (master's thesis, New Mexico State University, 2007) for studies on individual Service contributions.

<sup>3</sup> Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017), I-2.

<sup>4</sup> Bauer, *The Mexican War*, 194–195.

<sup>5</sup> House Executive Document 60, *Messages of the President of the United States, with the Correspondence, Therewith Communicated, Between the Secretary of War and Other Officers of the Government, on the Subject of the Mexican War*, 30<sup>th</sup> Cong., 1<sup>st</sup> sess. (Washington, DC: Wendell and Van Benthuysen, 1848), 1268–1269.

<sup>6</sup> Lloyd, "Serving in Obscurity," 24–26; Santelli, *Marines in the Mexican War*, 3; Stephen A. Carney, *Guns Along the Rio Grande: Palo Alto and Resaca de la Palma*, CMH Pub. 73-2 (Washington, DC: U.S. Army Center of Military History, 2005), 6.

<sup>7</sup> William A. DePalo, Jr., *The Mexican National Army, 1822–1852* (College Station: Texas A&M University Press, 1997), 96.

<sup>8</sup> Lloyd, "Serving in Obscurity," 32.

<sup>9</sup> Carney, *Guns Along the Rio Grande*, 5, 11–13.

<sup>10</sup> Bauer, *The Mexican War*, 54–57, 90–100.

<sup>11</sup> Lloyd, "Serving in Obscurity," 40–49.

<sup>12</sup> Bauer, *Surfboats and Horse Marines*, 165–166, 174–176.

<sup>13</sup> Winston Groom, *Kearny's March: The Epic Creation of the American West, 1846–1847* (New York: Vintage Books, 2012), 202–212.

<sup>14</sup> *Ibid.*, 223–226.

<sup>15</sup> Bauer, *Surfboats and Horse Marines*, 202–204.

<sup>16</sup> Stephen A. Carney, *Desperate Stand: The Battle of Buena Vista*, CMH Pub. 73-4 (Washington, DC: U.S. Army Center of Military History, 2008), 35–39.

<sup>17</sup> House Executive Document 60, 1271.

<sup>18</sup> Bauer, *Surfboats and Horse Marines*, 70–74, 79–82.

<sup>19</sup> *Ibid.*, 82; Bauer, *The Mexican War*, 245–253.

<sup>20</sup> Timothy D. Johnson, *A Gallant Little Army: The Mexico City Campaign* (Lawrence: University of Kansas Press, 2007), 84–97, 140, 239–241.

<sup>21</sup> Santelli, *Marines in the Mexican War*, 38–43.

<sup>22</sup> J. Jacob Oswandel, *Notes of the Mexican War, 1846–1848*, ed. Timothy D. Johnson and Nathaniel Cheairs Hughes, Jr. (Knoxville: University of Tennessee Press, 2010), 78.

<sup>23</sup> Nathan A. Jennings, *Riding for the Lone Star: Frontier Cavalry and the Texas Way of War, 1822–1865* (Denton: University of North Texas Press, 2016), 214–216, 230–232.

<sup>24</sup> Bauer, *Surfboats and Horse Marines*, 101–105, 117–121; Lloyd, "Serving in Obscurity," 75–82.

<sup>25</sup> Bauer, *Surfboats and Horse Marines*, 207–219, 222–233.

<sup>26</sup> Irving W. Levinson, *Wars Within War: Mexican Guerrillas, Domestic Elites, and the United States of America, 1846–1848* (Fort Worth: Texas Christian University Press, 2005), 98–99, 109–110.

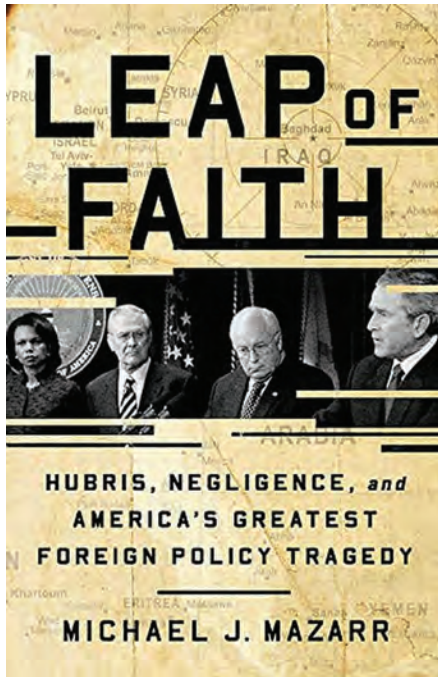
<sup>27</sup> JP 3-0, I-1.

<sup>28</sup> Winders, *Mr. Polk's Army*, 72; Santelli, *Marines in the Mexican War*, 3, 34.

<sup>29</sup> House Executive Document 60, 1271.

<sup>30</sup> JP 3-0, I-1.





## Leap of Faith: Hubris, Negligence, and America's Greatest Foreign Policy Tragedy

By Michael J. Mazarr

New York: PublicAffairs, 2019

512 pp. \$30.00

ISBN: 978-1541768369

Reviewed by Andrew J. Forney

Horror movies build fear through a series of formulaic events. A young couple drives into the dark woods, or a teenager, home alone, descends into a dimly lit cellar. No one ever checks behind the door—we all know what is coming next, but the outcome still scares us because, by knowing, tension has built. Sure, there may be a few jump scares, but for the most part we are not really surprised. We continue to watch, enthralled and unable to look away.

For a generation of national security professionals and military officers, reading about the run-up to the Iraq War can feel like watching a bureaucratic horror movie. After almost two decades, we know what is lurking behind the faulty assumptions, and reading ever more quickly, page after page, we wonder if this time the toxic brew of naivete and

hubris will not lead us down the tortured path that we know in our rational minds it will. Closing our books about that war—and Michael Mazarr's *Leap of Faith* is among the very best volumes—we almost want to scold ourselves: We fell for the same tricks, and we ended at the same frustrating place.

So why do we read these books? You might as well ask why we watch horror movies. Beyond providing entertainment and the thrill of being scared, horror movies wrestle with those things we do not like to talk about: fear, loneliness, and despair. For those who experienced the Iraq War, be they Soldiers, civilian professionals, or politicians, there remains a desire to understand similar, complex issues. From biased executive decisionmaking processes, through an over-militarization of foreign policy, to a national accounting for the events spawned by the American intervention in Iraq, Mazarr explores them all in *Leap of Faith*, confronting difficult subjects with an eye toward explanation. And, unlike many other books that share the “Modern Warfare” shelf at the bookstore, this volume reflects a more fulsome use of first-person accounts, not only from declassified materials but also from dozens of interviews with individuals who were there. Mazarr invested hundreds of hours gathering the day-to-day essence of the run-up to the war, and it shows. No other work on the early decision to go to war in Iraq benefits from a deeper bench of personal reflections.

These interviews and anecdotes outline the contours of a bipartisan National security momentum, defined by the pairing of a deep messianic tradition in American foreign policy with a driving belief in untrammelled American exceptionalism that defined the post-Cold War era. Mazarr shows how this momentum generated, gradually, its own certainty, one that framed global events into a Manichean “good vs. evil” bipolarity. The attacks on 9/11 catalyzed these beliefs, cementing the “us vs. them” predilections present in many senior leaders’ minds. A generational bias against Iraq, practiced by multiple Presidents and both political parties, allowed for a feat of near

prestidigitation: the shift of focus from Afghanistan to Iraq within days of the attacks in New York and Washington, DC.

In the process, avenues of discourse and dissent became closed off or were assumed away, leaving few means to “off-ramp” from a future war against Saddam Hussein and Baghdad. Behind this intellectual force, Mazarr further details the bureaucratic machinations that turned ideas into reality. Here he pulls no punches, heaping blame on then-Secretary of Defense Donald Rumsfeld and former Vice President Dick Cheney—not only for their policy biases and predilection toward military force but also, more important, for the way they managed the bureaucratic infighting to widen their fiefdoms within the interagency community, often for no other reason than to increase their political sway. Just as with the boogeyman under the bed, we as an audience know these biases are there, but fully seeing the implications they had, and how they absolutely subverted the National security process, remains disconcerting, nonetheless.

By adding recently declassified British accounts of the internal debates regarding the war, and the minutes from interrogations of senior Iraqi leaders (to include Saddam himself), *Leap of Faith* places what had been a decidedly American narrative in an international context. The disbelief, in both London and Baghdad, about the unchecked American drive toward war resonates throughout the book. As Mazarr points out, the United Kingdom had taken steps to account for its support and involvement in the Iraq War, something that he believes the United States still must do. Only by executing a formal accounting of the decisions that led to war in 2003, as per the British model, can we better understand the implications of the war on American politics, foreign policy, media, and society.

To this end, Mazarr apportions blame for the mistakes made between 9/11 and the start of the war in March 2003. Such a step is less akin to preparing to adjudicate punishment and more a recognition that adjudicating accountability can lead to understanding and,

eventually, reckoning. And while he does hold Rumsfeld and Cheney chiefly responsible for the events that befell the United States before and after the start of the war, he also realizes that limiting the discussion to this timeframe does not fully address the scope of the tragedy. The mistake to invade Iraq, as Mazarr sees it, has many fathers: a national security process driven by consensus over debate, a foreign policy that under-resources diplomacy, a media swayed by jingoistic arguments for war, and many others. Mazarr struggles to find discernment, and its practice, in American society.

*Leap of Faith* deserves a place on the bookshelf of every leader in the joint force and the National security policy community, alongside *Cobra II*, *The Assassin's Gate*, *To Start a War*, and the U.S. Army's recent retrospective volumes on the conflict to round out a full appreciation of the Iraq War. What Mazarr provides, and most other books on this subject do not, are several policy recommendations intended to provide alternative perspectives on international crises to senior leaders, keep pathways for discourse open, and prevent the overstepping of bounds within the inter-agency community and its collaborative processes. Although not all suggestions may be implemented, they come from a logically sound place and deserve further consideration. Mazarr realizes the difference between a horror movie and foreign policy decisionmaking. Here we can talk to the audience.

Here we can say, "Don't go in there." JFQ

---

Lieutenant Colonel Andrew J. Forney, USA, Ph.D., is a Strategist currently assigned to the Strategy and Force Development Branch within the Office of the Under Secretary of Defense for Policy.



### The Black Banners (Declassified): How Torture Derailed the War on Terror After 9/11

By Ali Soufan, with Daniel Freedman  
 W.W. Norton & Company, 2020  
 594 pp. \$17.95 (paperback)  
 ISBN: 978-0393343496

Reviewed by Bryon Greenwald

This declassified/unredacted version of Ali Soufan's 2011 edition of *Black Banners* is a must-read for anyone interested in terrorism, the psychology of interrogation, bureaucratic politics, and the lessons of poor leadership. Soufan demonstrates how dysfunctional U.S. intelligence services were before and after 9/11. He also demolishes the argument for the enhanced interrogation—or torture techniques—authorized by the George W. Bush administration and championed by the Central Intelligence Agency (CIA). *Black Banners* ranks with Steve Coll's *Ghost Wars* and Lawrence Wright's *The Looming Tower* as key sources for understanding al Qaeda.

Soufan presents a personal account of the Federal Bureau of Investigation (FBI)'s detective work that went into

uncovering attacks by al Qaeda and other terrorist groups. Although the book is generally chronological, Soufan weaves a tight narrative and freely jumps forward or backward in time to connect key events. A Lebanese American fluent in Arabic, Soufan joined the FBI on a bet with his college fraternity brothers; the United States is lucky he did. As Lawrence Wright notes, "Unfortunately, we have only one Ali Soufan. Had American intelligence listened to him, 9/11 might never have happened."

On that subject, Soufan is unsparing. The CIA knew in January 2000 that al Qaeda operatives, including two eventual 9/11 hijackers, had met in Malaysia. The CIA stated that "they knew nothing" when the FBI asked about this meeting in November 2000, April 2001, and July 2001. The CIA did not notify the FBI, the Immigration and Naturalization Service, or the Department of State that those hijackers also possessed U.S. visas. Thus, these men were not on any watch lists. They entered the United States and used their real names to get driver's licenses, open bank accounts, and buy tickets for American Airlines Flight 77, the airliner they later crashed into the Pentagon.

After 9/11, the lack of team play continued, as the CIA exerted new Presidential authority to interrogate terrorism suspects. Unfortunately, the CIA had mothballed its interrogation program and, according to Soufan, had no institutional expertise. Instead, the agency hired two contractors, James Mitchell and John Jessen, who claimed they could get detainees to "talk" by applying an ever-increasing menu of harsh techniques. The CIA paid them \$81 million, although they had never previously interrogated anyone or met an Islamic radical. That the Department of Justice and the White House sanctioned these techniques, even after Soufan proved them ineffective, signaled how seriously 9/11 traumatized the American policy apparatus and drove it to search for easy, if wrong, answers.

In newly declassified chapters, Soufan provides evidence of this trauma. In March 2002, the CIA asked Soufan to assist in interrogating Abu Zubaydah, the first high-level detainee captured by

the United States. While not a member of al Qaeda, Zubaydah was an important terrorist facilitator. The CIA captured Zubaydah, disguised and wounded, in a shoot-out. Initially, the agency could not identify him and did not dispatch any interrogators. When Soufan arrived in Thailand to assist, a CIA officer remarked that “We all work for Uncle Sam” and let Soufan question Zubaydah without the agency’s support.

Soufan began not by causing Zubaydah pain, but by calling him by the nickname his mother had given him, which quickly convinced Zubaydah to cooperate. Within an hour, Zubaydah confessed to an ongoing plot. Soufan relayed that information to CIA headquarters, which thwarted the attack. Surprised at how fast Zubaydah cooperated, CIA Director George Tenet wanted to congratulate his agents. When told the CIA team was absent and that Soufan had obtained the intelligence, Tenet was furious and ordered his team to take over.

Meanwhile, after a James Bond-worthy undercover trip to get Zubaydah to a hospital for lifesaving treatment, Soufan’s rapport-building paid off as Zubaydah identified a photograph of Khalid Sheikh Mohammed, verified his al Qaeda position, and credited him as the mastermind behind 9/11. When Mitchell took over, he stripped Zubaydah, exposed him to loud rock music, and kept him awake for 24 hours. Each time Zubaydah was instructed to “tell me what you know,” he was silent or asked, “What do you want to know?” After multiple failures, the CIA asked Soufan to restart the interrogation, which he did with notable success. But confirmation bias and bureaucratic zeal prevailed: Mitchell received new authorization for what were clearly experiments—not proven techniques—that included extended sleep deprivation, coffin confinement, and waterboarding. Zubaydah, who had trained to withstand worse, revealed nothing or simply lied to stop the torture.

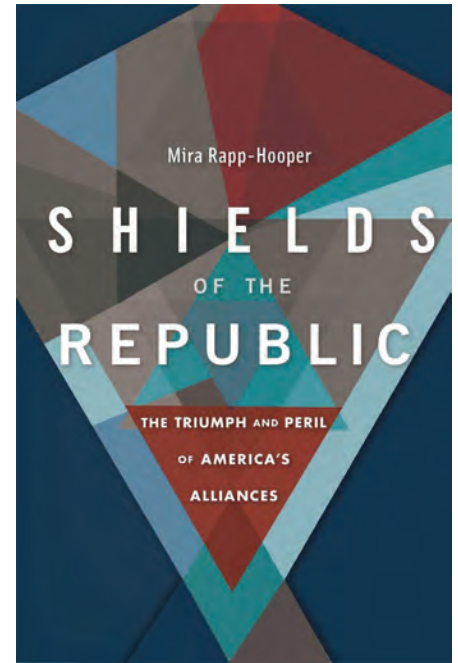
Lying also enabled the torture to continue. The CIA falsely touted its techniques, claimed credit for intelligence Soufan unearthed, and knowingly issued incorrect information. Despite

intelligence to the contrary, the CIA and the White House claimed that Zubaydah was the number 3 man in al Qaeda, but he was never a member. The CIA also maintained that after 30 to 45 seconds of waterboarding, Zubaydah gave up Jose Padilla, the supposed mastermind behind a plot to use a dirty bomb in an American city. In fact, the CIA waterboarded Zubaydah 83 times and obtained no new useful information. Zubaydah also confided that Padilla was not clever enough to mastermind anything. His supposed “plan” was to steal uranium from a hospital and swing it around his head in a bucket to enrich it. Perhaps most egregious was how the Bush administration linked Padilla, nuclear material, and Saddam Hussein together as it built a case to invade Iraq.

Some memoirists engage in self-delusion as to the value of their contributions. Soufan does not. Honestly written and corroborated by independent investigations into the torture of detainees, *Black Banners* is an extremely open, engaging history. It is essential reading for those who want to understand how al Qaeda and similar organizations operate, why torture does not work, and how ego and self-interest can cause leaders and those around them to abandon their principles. JFQ

---

Dr. Bryon Greenwald is Deputy Provost at the National Defense University.



### **Shields of the Republic: The Triumph and Peril of America’s Alliances**

By Mira Rapp-Hooper  
Harvard University Press, 2020  
272 pp. \$27.95  
ISBN: 978-0674982956

Reviewed by James J. Townsend, Jr.

The timing of Dr. Mira Rapp-Hooper’s book, *Shields of the Republic*, could not be better. In my many years as a civil servant in the Office of the Secretary of Defense, I would spend the first year of most new administrations explaining the North Atlantic Treaty Organization (NATO) to the incoming political appointees. Democrat or Republican, old Pentagon hand or neophyte, most knew something of NATO, but they arrived with some preconceived notions that were way off. That said, by the end of an administration, we usually had some real NATO pros among the appointees. Unfortunately, after a new administration took office, we would have to start all over again with the new batch.

Today, however, all my successor must do is hand *Shields of the Republic* to the new Biden appointees and walk away.

This book is not just about NATO; it covers U.S. alliance relationships globally—and crucially in the Asia-Pacific. Rapp-Hooper, an expert on Asia-Pacific security and a recently named senior advisor on China at the Department of State, provides important insight on China's rise and how the United States arrived late to understand the challenge we are facing today. According to Rapp-Hooper, alliances have never been more important as a way to address threats from Moscow and Beijing; however, with the rise of China's and Russia's turn toward aggressive, hostile behavior, the "Republic's shields are now in peril."

A highlight of *Shields of the Republic* is that it blends three key themes that readers would be wise to keep in mind as they contemplate alliances: the early U.S. experience with alliances (back to 1778) and how, but most important why, we broke with that experience to join NATO in 1949; the characteristics of alliances (how they work; how much they cost, both financially and politically; and the myths that surround them); and, finally, the relevancy of alliances today, especially after the Cold War and during this time of Great Power competition. She sounds the alarm that the West has much to do to adapt its alliance relationships in order to deter Russia and China today.

Rapp-Hooper points to an "incomplete post-Cold War transition" (a deeper dive into that transition would have been interesting) as the reason why today's alliance relationships in Europe and Asia are not up to the job of addressing new threats from Russia and China. She uses the term *competitive coercion* to describe Russia's and China's use of asymmetric, nonmilitary conflict and coercion to undermine alliances in ways that do not trigger treaty provisions. To deal with this new challenge, NATO and other alliance relationships must devise new strategies and adapt their tactics.

She also uses the 4 years of the Trump administration to test whether isolationism or transactional approaches to foreign relations is the right tactic for the United States. Her use of counterfactual analysis helps shine a light on what the world would be like for an America without

friends. Not to give her plot away, but Rapp-Hooper makes a winning case that America's alliances have been remarkably successful in protecting the Nation and that the charges of allies taking advantage of a naive United States is bunk. A point she makes throughout the book (and that I also saw countless times) is that "Washington spent more on defense than its allies but got far more out of its alliances than any one of them did."

At the same time, she urges the United States and its allies to avoid complacency when it comes to adapting to new challenges; failure to adapt will make alliances unable to withstand the stress of time and events. To help with this urgent task, her final chapter is full of meaty recommendations for NATO adaptation (some of which are already under way, such as including nonmilitary aggression as a trigger for Article 5), as well as ways to strengthen partners in Asia and to confront Chinese economic coercion.

I would take issue with some parts of this book, especially the view of Rapp-Hooper that Washington has "bifurcated the Alliance"—the United States can credibly support only the defense of Western Europe, but due to Russian local military advantages such as proximity, America "cannot be counted on to defend the Eastern European allies most in need of protection." The "unhappy choice" confronting NATO between escalation and giving in to the Russians during a quick, local Russian assault—a choice between catastrophe and shattering the Alliance—would cause the United States to hesitate. I do not believe for a moment that the United States and NATO would hesitate to defend Central and Eastern Europe, and, since Crimea, NATO and the United States have been building up forces and readiness in Europe to do so. The United States and NATO have put skin in the game by deploying what are essentially "tripwire forces" in each Baltic state (and Poland, which would also come under attack), guaranteeing a response. Rapp-Hooper's claim that "only local forces" are available to defend Baltic borders with Russia is not the case, and her use of a well-known

but outdated 2016 RAND study, *Reinforcing Deterrence on NATO's Eastern Flank*, to illustrate Baltic vulnerability should be reconsidered. Although her basic point that defending some allies from a quick Russian attack will be difficult, the cost of such an assault becomes higher for Russian forces each year and thus bolsters her case that Russia can be deterred if NATO is kept strong and credible. Rapp-Hooper's assertion that "without using force against the [A]lliance, Russia has eroded its unity and its capacity to assure members" would make for an interesting debate in the North Atlantic Council.

*Shields of the Republic* is an important and useful addition to the growing oeuvre dedicated to exploring how alliances work. This book will be especially helpful for those members of the joint force who are or will be working with allies in Europe or in Asia. Dr. Rapp-Hooper does a great job of myth-busting in a short and readable book that sets straight so many of the misconceptions held by those who come walking into the halls of government with every new administration. And she does more than just explain the problems that our alliances have today, she offers solutions that I hope find their way into practice. JFQ

---

James J. Townsend, Jr., completed a 34-year career in the Office of the Secretary of Defense as the Deputy Assistant Secretary of Defense for European and NATO Policy (2009–2017) and is now an Adjunct Senior Fellow at the Center for a New American Security.



Force Reconnaissance Marine with Command Element, 31<sup>st</sup> Marine Expeditionary Unit, sets security perimeter on starboard bridge wing during visit, board, search, and seizure exercise aboard amphibious dock landing ship USS *Germantown*, South China Sea, September 6, 2020 (U.S. Navy/Taylor DiMartino)

# Toward Military Design

## Six Ways the JP 5-0's Operational Design Falls Short

By Andrew L. Crabb

The day after Kabul fell to the Taliban, a combatant commander reportedly went to his J5 and told him to come back within 48 hours with data on the effects that the loss of Afghanistan would have on the future of military planning. While the veracity of this account cannot be directly verified, the rumor—and the speed at

which it spread—speaks to the coming scrutiny that joint planning is sure to undergo from multiple quarters. The refocus on strategic competition/crisis/conflict (among the United States, Russia, and China) and the rise of gray zone operations, along with the persistence of irregular warfare, all demand that our methodologies for conceiving and planning keep pace with the rapid evolution of our operation foci.

Joint Publication (JP) 5-0, *Joint Planning*, is the metronome for conceiving

and planning joint operations. It paces operational thinking and is the go-to resource for all joint force commanders, planners, task leads, and action officers. While JP 5-0 informs curricula at our intermediate-level education and advanced military studies institutions, it also crucially serves to inform and educate those who have not had the opportunity to receive intermediate-level education or advanced military studies. In many joint and unified commands, those individuals make up a sizable portion of typical joint planning groups, operational

---

Colonel Andrew L. Crabb, USMC (Ret.), is Professor of Operational Studies and Planning at the Joint Special Operations University.



Airman with Joint Task Force–Crisis Response speaks with families who await processing during evacuation at Hamid Karzai International Airport, Afghanistan, August 20, 2021 (U.S. Marine Corps/Davis Harris)

planning teams, and other boards, bureaus, cells, centers, and working groups. Therefore, it is vital that JP 5-0 remains relevant, practical, and creative.

Although the latest version of JP 5-0 (December 2020) has many laudable updates and improvements, the section of chapter 4 (on operational design) that addresses conceiving and expressing our operational ideas falls short in important ways. Simply put, to reach the lofty goals of understanding and addressing complex military problems, while preparing joint planners for the aforementioned challenges, chapter 4 of JP 5-0 must be redesigned and republished.

What follows are six key areas for revision; however, before exploring the shortfalls, we should make certain we understand both how JP 5-0 defines *operational design* and the methodology for its application.

## Background

In 2006, when JP 5-0 first added operational design to the planning publica-

tion, it was a huge step forward for joint doctrine. Operational design is envisioned both to precede and to complement the joint planning process (JPP). Whereas JPP applies “procedural rigor” to the planning process, operational design gives joint planners a more flexible tool to initially conceive prospective solutions for complex operational problems.<sup>1</sup> Per JP 5-0, operational design “provides a framework for coordinating the operations and activities of the joint force within space and time to achieve strategic objectives.” Since the introduction of JP 5-0, successive editions—up to and including the December 2020 edition—have continued to refine and improve the operational design concept.

The operational design methodology calls for planners to progress through the following steps:

- understand the strategic direction and guidance
- understand the strategic environment (for example, policies, diplomacy,

and politics) and the related contested environments

- understand the operational environment and relevant contested environments
- define the problem—that is, create shared understanding and plan for uncertainty
- identify assumptions needed to continue planning (for example, strategic and operational assumptions)
- develop options (for example, the operational approach)
- identify decisions and decision points (external to the organization)
- refine the operational approach(es)
- develop planning and assessment guidance.<sup>2</sup>

In other words, planners must understand the problem within their strategic- and operational-level milieu. They can then develop solutions, drawing on the 13 elements of operational design, to form an operational concept or “operational approach.”<sup>3</sup>

## Shortfalls of Operational Design

Now that we have a basic understanding of what operational design means in the JP, we should examine the six main shortfalls that limit the utility of the chapter on this concept.

**Shortfall 1.** Operational design does not educate joint members on the history or purpose of design.

**Result.** Planners unfamiliar with the background or purpose of design will not be able to fully grasp its creative application.

Design movements, sometimes called the applied arts, arose in the late 19<sup>th</sup> and early 20<sup>th</sup> centuries to infuse artistic expression and creativity into the dull industrial goods of the era.<sup>4</sup> The idea of creative processes preceding scientific engineering rapidly spread across many artistic and industrial communities. The goals and purposes of these design movements varied, but the common attribute was a desire to harness creativity and artistic expression to produce things that were beautiful, clever, and useful.

Architectural design, industrial design, and graphic design are a few movements that are at least somewhat familiar to the layperson. Many in the U.S. military, sparked by Israeli General Shimon Naveh, took up the design torch in reaction to what they saw as the limitations of the JPP and its cousins in the branches of the Armed Forces (for example, the U.S. Army's Military Decision-Making Process and the Marine Corps Planning Process). These limitations included a belief that JPP stymied creative thinking, promoted blind adherence to a process, and was a process that was inappropriate for complex, unclear, or unbounded problems.

A short introduction to the purpose and background of design and how operational design evolved from those early concepts would give joint planners of all grades and experience—especially those who have not attended advanced military schools—the necessary context to appreciate its purpose and application. Such an addition would inform and motivate planners as they move forward to creatively solve the daunting challenges that exist in the joint military domain.

**Shortfall 2.** Operational design does not educate joint planners on the nature of complex problems and problem-solving.

**Result.** Joint planners will not understand the attributes of complex problems and the general approaches to solving them.

At the joint level, military planners encounter challenges that are complex, diffuse, and opaque. In their groundbreaking 1973 work “Dilemmas in a General Theory of Planning,” Horst Rittel and Melvin Webber described such complex problems as “wicked.”<sup>5</sup> Wicked problems are characterized by “those complex, ever changing societal and organizational planning problems that you haven’t been able to treat with much success, because they won’t keep still. They’re messy, devious, and they fight back when you try to deal with them.”<sup>6</sup> Wicked problem sets (as opposed to “tame” or straightforward problem sets) defy easy characterization; solutions are unapparent and elusive, and the challenge itself may even be intractable (conditions changed, but the problem never truly resolved). Often, they are problems that reside in and among human societies and the networks of the human domain. These networked difficulties have links among and between one another that produce direct second- and third-order effects and indirect cascading, compounding, and cumulative effects.<sup>7</sup>

Joint military problems could arguably be among the most wicked problems that humans encounter. In the joint community, action officers are often told to analyze and propose solutions to myriad wicked problems. Just a few examples could include situations as diverse as planning in a time-sensitive crisis, deliberate planning in development of a new regional campaign plan, establishing a partner-nation’s navy, reorganizing a joint command or directorate, or even reconciling two opposing factions in an assigned area of responsibility. All take place in the human domain and deal with complex, fluid, and interconnected problems that may not have a readily apparent solution.

Chapter 1 of the new JP 5-0 dedicates four paragraphs to the topic of

“understanding problems” but is mainly focused on constructing a “problem statement.” Chapter 4 dedicates quite a bit of discussion on how to dissect and analyze the environment that houses the problem. These inclusions are commendable, but our problem-solvers must understand the characteristics and leading scholarship of complex problems and general approaches to problem-solving.<sup>8</sup> Another short section on the topic would greatly improve chapter 4.

**Shortfall 3.** Operational design does not educate joint problem-solvers on creative thinking and cognition.

**Result.** Joint planners will not understand how individuals think, how groups collaborate, and how both are often captive to perspectives and biases.

As noted when discussing the previous shortfall, joint force commanders expect planners to be doctoral-level problem-solvers. Unfortunately, we are asking our planners to think individually and facilitate thinking at the group level without first educating them on the traits of individual and group cognition. There are whole disciplines dedicated to cognitive psychology, design, and problem-solving. A short addition to chapter 4 should include topics such as intuitive vs. cognitive decisionmaking, understanding how biases skew perspectives, cognitive dissonance, the value of intellectual empathy, and even on arcane but interesting topics such as the principles of Gestalt theory.<sup>9</sup> By thinking about thinking, our planners and problem-solvers would be better prepared individually and collaboratively to lead groups through the cognitive hurdles of joint problem sets.

**Shortfall 4.** Operational design does not incorporate stratagems and deception as one of its components.

**Result.** Joint planners will undervalue the use of operational-level deception; planners will be unable to anticipate, identify, and forecast our adversaries’ deception.

The beginning of chapter 4 outlines operational art and the elements that commanders and staff wield in its application. *Operational art* is “the cognitive approach 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, means, and risks.”<sup>10</sup> If operational art is the synthesis expressed in warfare’s application, then the guideposts that structure such thinking are the elements of operational design. Unfortunately, the 13 elements of operational design contain no references to stratagems, deception operations, operational artifices, or military ruses. The idea of confusing the enemy as to our true aims and intentions is entirely absent in the stages of operational conception. At the operational level, actions in the operational environment and military information support operations that use stratagems and deception. The intent is that they lead the enemy to take actions that favor our own ends. Deceiving our enemies and obscuring our intent is a mindset that needs to be developed in all joint force commanders and staffs. Application should happen early in the conception of a campaign, not added as an afterthought or merely a checked box or used as an operational band aid. Although the Joint Staff has placed enough importance on military deception to devote an entire publication to it (JP 3-13.4, *Military Deception*<sup>11</sup>), JP 5-0 does not include deception in the operational design process.

Our adversaries clearly understand its import—Russian General Valery Gerasimov’s “New Look” doctrine incorporates deception and denial at every level of warfare (for example, the “little green men” who took over the Crimea in 2014).<sup>12</sup> China’s People’s Liberation Army has been long known to incorporate Sun Tzu’s theories into its unrestricted warfare doctrine, including the mantra that “all warfare is based on deception.”<sup>13</sup> Our military planners should understand that, in every aspect of warfare, stratagems and deception are foundational concepts that must always be considered in the design of our operations. Give stratagems and deception the consideration they deserve by making them elements of operational design so that they are correctly promoted in operational thinking, theory, and the

nascent stages of our commanders’ and staffs’ planning efforts.

**Shortfall 5.** Operational design is focused on solving operational problems.

**Result.** Joint planners will not be equipped to resolve nonoperational problem sets.

In a military planning manual, it seems only logical that the authors would present a methodology centered on military operational planning. In the real world of military staff work, joint planners are presented with innumerable complex problems that are not centered on a military operation. Joint force commanders and planners are often tasked to design solutions to address such wicked problems as poverty, lack of a training regimen, and conflict resolution. These are just the tip of the wicked military problem iceberg. Our military problem-solving doctrine (as currently expressed in JP 5-0’s chapter 4) should be broad and flexible enough to allow our planners to assess and reason through any complex problem.

**Shortfall 6.** Operational design promotes an “operational approach” process that is inadequate for complex operational environments.

**Result.** This methodology will work well only for binary force-on-force operations in ordered environments.

The operational design process outlined in JP 5-0 culminates in the production of an “operational approach.”<sup>14</sup> Simply stated, the operational approach is the joint force commander’s concept of the operation. JP 5-0 devotes limited discussion to how joint force commanders and planners develop an operational approach, implying that commanders and planners can tap into the “elements of operational design” to conceive one. Chapter 4 does provide a tool for developing an operational approach: the center of gravity (COG) analysis.<sup>15</sup> In a state-on-state conventional conflict, in an ordered operational environment, the COG methodology works well to identify the enemy’s main strength and the critical factors that underpin it. In this situation, the COG identification and analysis is an invaluable means that can lead to the conception of a valid operational approach to defeating the adversary and

achieving the endstate. Unfortunately, the COG process has limited usefulness when it comes to facing and accounting for multiple adversaries, neutral parties, and unknown actors in a disordered and chaotic operational environment.

The COG process assumes that defeating an armed adversary is the central obstacle to achieving the desired endstate. In disordered and chaotic operational environments, defeating an armed adversary may at best be beside the point and at worst counterproductive. In such a situation, centering an operation on the destruction or neutralization of multiple adversaries’ COGs could simply inject more chaos and complexity into a fractured system (for example, Mexico’s “war” on its drug cartels<sup>16</sup>). The 2017 JP 5-0 correctly mentioned that COGs exist only for “unitary systems” and also noted that irregular warfare may lead to different analyses about where to focus efforts.<sup>17</sup> While leaving out a detailed examination of ordered vs. disordered environments and references to irregular warfare, the 2020 JP 5-0 does correctly note that “without a well-defined threat, there will often be no enemy or adversary COG.”<sup>18</sup> Unfortunately, the discussion ends there, offering no further guidance for developing operational concepts in these irregular problem sets.

JP 5-0 should keep the COG methodology for binary operational problems, but it needs to address where the COG methodology is appropriate and where it may prove limited or detrimental to our objectives. It also needs to speak clearly and plainly to the challenges of operations in chaotic operational environments and irregular operational problems.

## The Solution to the Shortfalls

If we accept that the six shortfalls are valid, then it is clear we need to redesign and republish JP 5-0’s chapter 4. We must not focus solely on operational problem sets; instead, we should adopt a flexible system that encourages creativity, while also developing implementable, practical solutions. In short, we need “military design.”

Military design would provide context on the background of design, educating readers on the nature of complex





Airmen with 5<sup>th</sup> Aircraft Maintenance Squadron push open B-52H Stratofortress bomb bay door to load weapons, December 7, 2021, at Edwards Air Force Base, California (U.S. Air Force/Michael A. Richmond)

problems and how people reason to resolve them. It would foster creative and practical solutions (for example, incorporation of military deception). Military design would not be limited to solving binary, operational planning problems; instead, it would discuss the planning and problem-solving methods for a wide variety of conventional and irregular operational problem sets. Finally, because military design would be open-ended and flexible, it would enable joint planners to reason through both operational and nonoperational problems.

There are truly dozens of ways to express different design processes. We already have the JPP—do we really need another lengthy, linear, and iterative process? Is there another way we can encourage creative thinking?

A simplified, open-ended problem-solving practice would harness the creative and cognitive abilities of our planners. Like Archimedes in his laboratory, planners—via continuous conscious and unconscious introspection and possibly

through collaborative exploration of the problem—eventually could have their own eureka moment and devise a solution. Building on my previous thoughts on operational design, I would advance that military design be considered a *practice*, not a linear process.<sup>19</sup> In other words, military designers should continuously assess and reassess the problem through what may be five key elements of problem-solving. Planners can visit and revisit these cognitive vantage points sequentially or as the planner gains insights into each:

- contextualize the problem
- conceive the desired condition or outcome
- identify sources of resistance to achieving the outcome
- identify ways to mitigate resistance sources
- express the solution.

JP 5-0's updated chapter 4, "Military Design," could and should keep the excellent contextual information on operational planning while addressing

all the previously mentioned shortfalls. The result would be a military design practice that is simple yet broad enough to address any challenge: operational problems (symmetrical/ordered and asymmetrical/disordered), nonoperational problems, clearly defined problems (told what to do but not how to do it), and opaque and wicked problems (no agreement on the issue's makeup or way forward). The result would be an exponential improvement in joint problem-solving. It would inspire and fire the creative energies of joint force commanders and planners. The only question that remains is should we rename JP 5-0 as *Problem Solving & Planning*. JFQ

## Notes

<sup>1</sup> Joint Publication (JP) 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), III-4, available at <[https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5\\_0.pdf?ver=us\\_fQ\\_pGS\\_u65ateysmAng%3D%3D](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf?ver=us_fQ_pGS_u65ateysmAng%3D%3D)>.

<sup>2</sup> JP 5-0, IV-2–IV-3.

<sup>3</sup>The 13 elements of operational design are objectives, military endstate, center of gravity, effects, culmination, lines of operation, lines of effort, decisive points, direct and indirect approach, operational reach, arranging operations, anticipation, and forces and functions. See JP 5-0, III-75, fig. III-23.

<sup>4</sup>Deborah Ascher Barnstone, *Beyond the Bauhaus: Cultural Modernity in Breslau, 1918–33* (Ann Arbor: University of Michigan Press, 2016), 81–107, available at <doi.org/10.2307/j.ctt1gk088m.7>.

<sup>5</sup>Horst W.J. Rittel and Melvin M. Webber, “Dilemmas in a General Theory of Planning,” *Policy Sciences* 4, no. 2 (1973), 155–169.

<sup>6</sup>Tom Ritchey, “Wicked Problems: Modelling Social Messes with Morphological Analysis,” *Acta Morphologica Generalis* 2, no. 1 (2013), available at <[https://www.researchgate.net/publication/236885171\\_Wicked\\_Problems\\_Modelling\\_Social\\_Messes\\_with\\_Morphological\\_Analysis](https://www.researchgate.net/publication/236885171_Wicked_Problems_Modelling_Social_Messes_with_Morphological_Analysis)>.

<sup>7</sup>Edward C. Mann III, Gary Endersby, and Thomas R. Searle, *Thinking Effects: Effects-Based Methodology for Joint Operations* (Maxwell Air Force Base, AL: Air University Press, October 2002), available at <[https://media.defense.gov/2017/nov/21/2001847048/-1/-1/0/cp\\_0015\\_mann\\_endersby\\_searle\\_thinking\\_effects.pdf](https://media.defense.gov/2017/nov/21/2001847048/-1/-1/0/cp_0015_mann_endersby_searle_thinking_effects.pdf)>.

<sup>8</sup>Foundation for Critical Thinking Web site, available at <<https://www.criticalthinking.org/>>.

<sup>9</sup>Max Wertheimer, with a foreword by Kurt Riezler, “Gestalt Theory,” *Social Research* 11, no. 1 (February 1944), 78–99.

<sup>10</sup> JP 5-0, IV-1.

<sup>11</sup> JP 3-13.4, *Military Deception* (Washington, DC: The Joint Staff, January 26, 2012), available at <[https://jpsc.ndu.edu/portals/72/documents/jc2ios/additional\\_reading/1c3-jp\\_3-13-4\\_mildec.pdf](https://jpsc.ndu.edu/portals/72/documents/jc2ios/additional_reading/1c3-jp_3-13-4_mildec.pdf)>.

<sup>12</sup>David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford Press, 2020), 163.

<sup>13</sup>Sun Tzu, *The Art of War* (New Delhi: Diamond Pocket Books, 2021), 6.

<sup>14</sup> JP 5-0, IV-14.

<sup>15</sup> JP 5-0, IV-25, fig. IV-8.

<sup>16</sup>“Mexico’s Long War: Drugs, Crime, and the Cartels,” Council on Foreign Relations, February 26, 2021, available at <<https://www.cfr.org/backgrounder/mexicos-long-war-drugs-crime-and-cartels>>.

<sup>17</sup> JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, revised June 16, 2017), IV-43.

<sup>18</sup> JP 5-0, IV-24.

<sup>19</sup>Andrew “Buster” Crabb, “Joint Operational Design, Re-Imagined . . .,” *Small Wars Journal*, October 26, 2020, available at <<https://smallwarsjournal.com/jrnl/art/joint-operational-design-re-imagined>>.

## Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 3-01, *Countering Air and Missile Threats*

JP 3-03, *Joint Interdiction*

JP 3-15, *Barriers, Obstacles, and Mine Warfare in Joint Operations*

JP 3-20, *Security Cooperation*

JP 3-25, *Countering Threat Networks*

JP 3-33, *Joint Task Force Headquarters*

JP 3-42, *Joint Explosive Ordnance Disposal*

JP 3-52, *Joint Airspace Control*

JP 3-68, *Noncombatant Evacuation Operations*

---

## JPs Revised (signed within last 6 months)

JP 2-0, *Joint Intelligence*

JP 3-0, *Joint Campaigns and Operations*

JP 3-04, *Information*

JP 3-07, *Joint Stability*

JP 3-35, *Joint Deployment and Redeployment Operations*

# CALL FOR ENTRIES

for the

2022 Secretary of Defense and  
2022 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 2021–2022 academic year. Students are encouraged to begin early and avoid the spring rush. Final judging and selection of winners take place May 12–13, 2022, 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

### Strategic Assessment 2020: Into a New Era of Great Power Competition

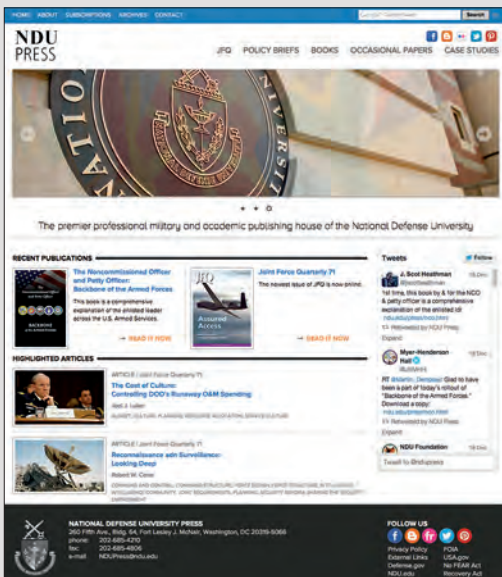
Edited by Thomas F. Lynch III

Great Power competition is a framework for understanding interstate relations that dominated geopolitics for centuries prior to World War II. Past GPC eras have featured multiple powerful states jockeying for relative status and position. After lying dormant during a two-decade period of post-Cold War globalization and American international primacy, the dynamics of GPC returned to international relations and security studies in earnest during the late 2010s.

*Strategic Assessment 2020* provides an expert and nuanced understanding of the most important emerging dimensions of GPC between the three Great Powers in 2020: the United States, China, and Russia. It establishes that the United States stands atop the triumvirate, with China a rising competitor and Russia vying for top-level prestige while facing clear signs of decline. The Sino-American competitive dyad is likely to be the dominant Great Power rivalry into the future. Chapters focus on the critical activities among these Great Powers and develop major implications for other state actors, nonstate actors, and global institutions.

Authors include scholars from the National Defense University and the Institute for National Strategic Studies who have been directly engaged as thought leaders and policymaking pioneers grappling with the strategic contours of the new era of GPC. Chapters and combinations of chapters will be not only useful for students of national security, international relations, and foreign affairs in an academic setting, but also of great value to policy practitioners.

## Have you checked out NDU Press online lately?



With 40,000 unique visitors each month, the NDU Press Web site is a great place to find information on new and upcoming articles, occasional papers, books, and other publications.

### You can also find us on:



Facebook



Flickr



Twitter



Pinterest

Visit us online at: <https://ndupress.ndu.edu>



# JFQ

JOINT FORCE QUARTERLY

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press  
National Defense University, Washington, DC

