JFQ | Joint Force Quarterly

Issue 95, 4th Quarter 2019

Maximizing Strategic Foresight

Why Normandy Still Matters

2019 Essay Competition Winners

Joint Force Quarterly

Founded in 1993 ▪ Vol. 95, 4th Quarter 2019
http://ndupress.ndu.edu

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

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

Executive Editor
Jeffrey D. Smotherman, Ph.D.

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

Internet Publications Editor
Joanna E. Seich

Copyeditor
Andrea L. Connell

Associate Editor/Book Review Editor
Jack Godwin, Ph.D.

Associate Editor
Patricia Strait, Ph.D.

Intern
Noah W. Garber

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

Cover 2 images (top to bottom): Air Force pararescueman assigned to 83rd Expeditionary Rescue Squadron communicates with Army Task Force Brawler CH-47F Chinook during training exercise in Afghanistan, March 14, 2018 (U.S. Air Force/Gregory Brook); U.S. Marines with 24th Marine Expeditionary Unit hike to cold-weather training site inland, Iceland, October 19, 2018, during Trident Juncture 18 (U.S. Marine Corps/Menelik Collins); Soldiers assigned to 2nd Battalion, 32nd Field Artillery, 1st Brigade Combat Team, 101st Airborne Division fire M777 howitzer on Qayyarah West Airfield, Iraq, August 10, 2019 (U.S. Army Reserve/DeAndre Pierce)

In This Issue

Forum

Essay Competitions

JPME Today

Commentary

Features

Recall

Book Reviews

Joint Doctrine

About the Cover
Aviation boatswain's mate (equipment) Airman Heaven Alexander secures lube line to port cylinder of catapult four on flight deck of Navy's only forward-deployed aircraft carrier, USS *Ronald Reagan*, Yokosuka, Japan, August 14, 2016 (U.S. Navy/Nathan Burke)

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.

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

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

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

4th Quarter, October 2019
ISSN 1070-0692

During Berlin Crisis of 1961, group of U.S. Naval Reservists talk to U.S. Army Soldiers who man Checkpoint Charlie, only American checkpoint along Berlin Wall (U.S. Navy Museum)

Executive Summary

This year has been one of important anniversaries and one of change. Just this past weekend, the world marked the 100th year since the Armistice for World War I, the "war to end all wars," was placed in effect. On that date, at the 11th hour of the 11th day of the 11th month, the bloodiest war up to that time ended. Or so the world had hoped. Just 25 years later, Allied forces would assault the beaches and skies above Normandy, France, in an unprecedented invasion to roll back the Nazi empire, which, along with Russian victories on the Eastern Front, would ultimately end that violent period in Western Europe. But that effort would eventually turn into the Cold War, a long struggle between U.S.-led Western powers and Soviet bloc countries. The 30th anniversary of the end of that conflict was marked this year, as the Berlin Wall ceased to function as a political and physical barrier between the German Democratic Republic (GDR) and West Germany on November 9, 1989, although official destruction of the wall did not begin until June 13, 1990.

And the anniversaries where we can honor our fallen and celebrate those who survived continue to reverberate. Lest we forget. But what can we say we have learned from this seemingly endless cycle of struggle that results in war? One answer has been to improve how our troops fight together as part of a joint force. To do so, its leaders need to understand the past, both good and bad, and find ways to make our joint bonds strong enough to meet the challenges ahead, even those that may surprise us.

I would offer that our world is in constant motion, and as a result change is what we must always seek to adjust and improve our situations. If you have a setback, a delay, or a loss, you do as the unofficial slogan of the U.S. Marine Corps suggests—you improvise, adapt, and overcome. I would add that we need to be constantly learning both from what we see and from what others experienced. As former Secretary James Mattis asked our professional military education (PME) institutions to do, developing our critical thinking skills and testing our intellectual limits in new and engaging ways are no longer options for a select few. To that end for the joint force, *Joint Force Quarterly* continues to offer discussions about past conflicts and current issues and to frame future concepts and issues in ways that hopefully help each of us better use our minds. With that as a goal, we offer a wide range of ideas to help you keep your intellectual edge. Hopefully, you will read them and send us your best ideas on how to keep improving the joint force.

In the Forum section we have three valuable perspectives on strategic issues. In reviewing the largest element of one of our important international partners, Emily Bienvenue and Zachary Rogers discuss some available opportunities for the Australian army to meet the complex and increasingly challenging threat environment there. Helping us in the world of teaching future strategic leaders, Amy Zalman offers advice on how we can get the most from strategic foresight. As threats seem to be multiplying as the 30th anniversary of the Cold War ends, Paul Stockton offers his view on how we can seek to identify issues and potential paths to successfully continuing our military missions in this difficult world.

This year's Secretary of Defense and Chairman of the Joint Chiefs of Staff (CJCS) Essay Competitions featured a record number of entrants from across the PME community. I want to thank all the judges and entrants for their participation and for once again accepting the challenge of determining the best expressions of ideas from those who are our future security leaders. Daniel Hooey's winning essay in the Secretary of Defense Strategic Research Paper category provides an interesting look at Pakistan's military stance and reliance on nuclear weapons. Speaking to the strategic issues of the security environment in the Pacific, the winning CJCS Strategic Essay Competition (Strategic Research Paper category) by Andrew Rhodes develops a new view of how U.S. power should be used to counterbalance China. And James B. Cogbill, winner of the CJCS Strategic Essay Competition (Strategy Article category) competition, suggests the experiences of Morocco in countering terrorism offers the United States a potentially superior approach to this threat.

In our JPME Today section, Bryon Greenwald, one of our leading professors and an award-winning historian who was instrumental in adding an overseas experience to the Joint Advanced Warfighting School in Norfolk, discusses the value of a student-led, student-focused battlefield history experience within that program and how similar offerings have a positive impact on our PME programs.

In Commentary we present two unique views on modern war, both past and future. As the 20th anniversary of the North Atlantic Treaty Organization war over Kosovo is marked, Phil Haun, one of the U.S. Air Force veterans of that conflict and now a historian and Naval War College dean, offers his thoughts on what he experienced then as a fighter pilot and later, after becoming a historian. Confronting conflict below the traditional levels of armed combat is the focus of an important set of ideas from Vayl Oxford, as he offers his take on dealing with 21st-century threat networks.

We are fortunate to bring you three distinctively refreshing articles in Features that span from internal improvement suggestions for fostering better jointness and joint operations to separate pieces on two of the five concerns of our National Security Strategy. Dina Eliezer, Theresa K. Mitchell, and Allison Abbe discuss how the military might develop its officers using more than what is required by the current Joint Qualification System. Additive manufacturing—also known as 3D printing—has started to revolutionize a growing number of areas, including the military, and Jaren K. Price, Miranda C. La Bash, and Bart Land describe how it could improve joint operations. Justin Roger Lynch delivers a valuable case study in military innovation by explaining how British scientists created the Chain Home early warning radar system, the world's first integrated air defense system.

One of the constant challenges in my job is finding useful history articles for our Recall section that provide valuable insights into joint operations. But somehow, we get a really great piece for you every issue. You may have initially scratched your head trying to see how last issue's Civil War article (*JFQ* 94 [3rd Quarter], "Flanking the Crater," by John K. DiEugenio and Aubry J. Eaton) fit that requirement, but after reading it, I hope you saw its value for modern joint warriors. This time we go even further back in history as Joseph Finnan, Lee Gray, John Perry, and Brian Lust help us understand joint principles through the lens of the Quebec Campaign of 1759. Along with three informative book reviews and our Joint Doctrine Update, in our Joint Doctrine section Matthew Florenzen, Kurt Shulkitas, and Kyle Bair help us work out the range of likely impacts of artificial intelligence on joint warfighting.

While change is a challenge for the joint force, NDU Press and your *JFQ* team is not immune. After serving as one of our associate editors for the past several issues, we wish Patricia Strait all the best in her well-earned retirement after many years in U.S. Government service. We also want you to know that NDU Press has moved its operations to the second floor of Marshall Hall here at Fort Lesley J. McNair, back to where we were more than a decade ago. Moving a team of eight along with 10 tons of books and equipment caused a bit of delay to our production process, but we hope you will come visit us in our new home. In the meantime, we look forward to publishing the very best ideas from, for, and about the joint force for many years to come. **JFQ**

William T. Eliason
Editor in Chief

Marine keeps watch during Talisman Sabre exercise, Shoalwater Bay Training Area, July 16, 2019 (Australian Defence Force/Jake Sims)

Strategic Army

Developing Trust in the Shifting Strategic Landscape

By Emily Bienvenue and Zachary Rogers

While the nature of war remains a battle of political wills, discontinuous change in the strategic landscape is constantly changing the way in which warfare is conducted.[1] Expedited by the speed and scope of technological change, the age of information warfare (IW) is well upon us.[2] While the impact of technological change on operational and strategic maneuverability in the physical battlespace is comparatively well understood, the impact of complex interwoven technological and social trends on the nature of conflict and the threat posed to the rules-based global order are less so.

The intentions of this article are twofold. First, it aims to improve understanding of the nature of change in the operating environment. Emerging from technological change is a strategic war against trust—trust in the open rules-based system and the sociopolitical systems of its key players. Authoritarian states such as China and Russia, for whom a level of revision of the existing order is a key strategic interest, are contending to rewrite, disrupt, or block the preferred narratives of the Western liberal democracies such as Australia's by sowing seeds of distrust within and without of their hyper-connected societies. Four interlocking features of the emergent operating environment

Emily Bienvenue is a Senior Analyst in the Joint Operations and Analysis Division at the Defence Science and Technology Group Edinburgh. Zachary Rogers is a Research Lead in the Jeff Bleich Centre for the U.S. Alliance in Digital Technology, Security, and Governance at Flinders University.

drive this change: the shift from vertical to horizontal networks of power, expansion of the cognitive battlespace, constant and unrestricted warfare, and the erosion of trust in traditional centralized institutions. In the digital era, state and nonstate actors alike exploit and manipulate information for commercial and strategic effect. Power flows among a diversity of actors connected through horizontal networks, in which the state's—and other traditional institutions'—roles and capacities to channel that power are disrupted.[3] The lines between the civilian and military domains and the conditions of peace and war are indistinguishable. The contemporary canter of warfare, considered as both violent and nonviolent contending with others for political gain, is now a constant between and across whole societies.[4] Chaos and disorder in the information domain undermine functionality in the Western liberal institutional tradition and degrade the basis of authority, legitimacy, and trust in the rules-based order.[5]

Second, this article asserts that trust, characterized by its relational nature, is the connective tissue that provides legitimacy and authority to the promise and functionality of openness and rule-making. It enables the acceptance of a level of vulnerability associated with open systems.[6] This relational trust offers us an advantage over adversaries that cooperate on a more transactional and calculative basis, and is thus an underrecognized strategic resource. Without trust and the normative principles and institutions that provide a plausible narrative for the rules-based global order, those who support and benefit from an open system risk strategic defeat below the threshold of conventional conflict.[7] To default to the employment of the offensive strategies of our adversaries, what Joseph Nye has termed "sharp power,"[8] is to risk forfeiting one of our most valuable strategic resources.[9] In addition, it is to play into the strategic strengths of adversary actors for whom the incumbent international order and its underpinnings of relational trust between allied partners are the primary competitive threat.

Shifting Contours of the Strategic Landscape

In 2004, the Australian army released a future operating concept. Written by Lieutenant Colonel David Kilcullen, "Complex Warfighting" described a "changing landscape in which [globalization] has created and empowered a diverse range of enemies of the west; and U.S. dominance . . . has caused those adversaries to seek asymmetric arenas and unconventional means to confront the west." Kilcullen's analysis of the operating environment and the evolving character of warfare centered around four longstanding trends: complexity, lethality, diversity, and diffusion of warfare. For Kilcullen, however, ongoing changes in the operating environment and the nature of warfare resided "in the unpredictable, ambiguous, and highly complex manner in which the trends interact, not in each trend itself."[10] Subsequent doctrine sketched the contours of such complexity, describing an operating environment "that is more than the physical environment."[11] However, the ongoing preoccupation with the modernization of technology as a means to maintain relative advantage in the physical battlespace neglects the deeply complex social changes Kilcullen was referring to.

Drawing on lessons from Iraq and Afghanistan, in 2006 Robert Scales purported that victory in the wars of the future would be decided by human and cultural factors. According to Scales, Iraq and Afghanistan indicated that it would be not technological superiority but rather the capacity to capture the perceptions and minds of populations that would determine victory on the battlefield.[12] The idea that war is not simply an engineering problem is not new. Scales goes beyond this understanding of warfare, claiming that human and cultural factors are decisive factors in battle. Indeed, close combat capabilities would remain a key function of an army that would have to contend with violent conflict; however, these capabilities would be insufficient to achieve strategic effect in the future war for minds.

Today, major shifts in the strategic landscape suggest that the narrative of liberal internationalism and the associated global governance model is under great strain. In place since 1945, the rules-based global order has been underwritten by the primacy of U.S. material power and principles of democracy, transparency, and openness as reflected and reinforced by national and global institutions. These pillars of the postwar order do not exist in isolation. Superior military and economic resources manifest as strategic power only when translated through the institutions able to convert the resource into the preferred strategic outcome. The capacity for the translation of resources into preferred strategic outcomes has been dependent on not only the maintenance of material superiority but also the sustainment of the enabling narrative.[13]

Through a combination of relative decline in material superiority and accumulating challenges to the narrative, the capacity for translation has been eroding for the United States for some time, marked by many scholars of the international order as far back as 1973 and beyond.[14] This decline has continued and accelerated in recent times, as major signs of fragility in the order marked by financial crises, breakdown of international consensus and cooperation, and security crises have proliferated since 2001. In addition, the digital age has ushered in new threats that have not only created a new terrain of competitive interactions but have also distorted existing orientations regarding competition and conflict. A major development has been the capacity of opponents of the existing order to cause disruption and dysfunction in its supporting narrative while pursuing material gains in other ways.[15]

Russian interference in the 2016 U.S. Presidential elections marks the manifestation and convergence of these trends. Fragility in the global order has given way to upheaval. As major reorientation of the global order is under way, states are being forced to adapt to the rapidly changing environment while seeking to preserve features of the order aligned with their strategic interests. For Australia, its interests remain tied to the material superiority

Iraqi security forces conduct wreath-laying ceremony at Tomb of Unknown Soldier as part of Third International Conference to Counter Daesh Propaganda and Ideology, in Baghdad, Iraq, December 13, 2017 (U.S. Army/Von Marie Donato)

of allied military and economic resources coupled with an institutional narrative of openness to cross-border trade and investment, the preservation of stability and security, and an emphasis on consensual and rules-based international governance. While global shifts in material power are forces outside of Australia's control, the sustainment and propagation of its preferred institutional narrative can be significantly influenced by whole-of-government actions.

This process is dependent on trust. It is trust that allows both individuals and states to commit to institutions in an environment of imperfect information and underpins the narratives that sustain them over time. Disinformation and uncertainty in the age of cognitive warfare present a direct threat to these processes and capacities to maintain and renew the institutions and norms that underwrite the rules-based global order.[16] Adversarial attempts to precipitate the erosion of trust are an attack on the connective tissue of allied strategic power. The erosion of trust must not be met with a retreat from trust; rather, it brings to the fore the centrality of *relational* trust as a strategic resource of allied systems and the paucity of trust in adversary systems.[17] Relational trust cultivation is the counter to adversary *transactional*-based relationships, which represent a vector of long-term strategic advantage that requires greater acknowledgment.

Nathan Freier and Jonathan Dagle of the U.S. Army War College have identified the challenge presented by an era of hyper-competition to the values of openness and liberalism:

> *Russia and China create the worst possible Faustian choices for U.S. public- and private-sector leaders. On the one hand: choose to stick to the core values that define the United States—a rules-based international order, truth and candor, free speech, free markets, free enterprise, etc.—and see those values exploited at U.S. expense. On the other hand: compromise those values to wrestle in the mud with rivals, and hazard erosion of the hard-won principles that have for so long separated the United States and other liberal democracies from their authoritarian adversaries.*[18]

This challenge is evident across a number of theaters of below-the-threshold conflict around the world. Gregory Poling reports on China extending its influence in the South China Sea not through its often cited military modernization but through its "weaponized" counter-narrative of victimization at the hands of European and Asian powers.[19] Digital platforms provide new opportunities for China to transmit this narrative not only to its domestic population but also to the region and beyond. China's narrative depicts the United States and its allies as a destabilizing force in the region and serves to propagate the belief that the U.S.-led security architecture, long synonymous with a rules-based global order, is merely a euphemism for its hegemony, not a guarantee of security and stability for the region.

A more unilateralist foreign policy under Trump and a reduction of U.S. hard power in the region play to China's counternarrative. This metanarrative provides a façade for the People's Liberation Army's incremental territorial gains in the South China Sea. By targeting the morality of U.S. strategy, it challenges the normative basis for the "rules-based global order" without which the United States and other members of the regional system of alliances, most notably Australia, cannot exercise their material power. As noted by U.S. Air Force Intelligence and Information Operations Officer Jon Herrmann, "When a narrative, as a key example of information power, falters, other forms of power also falter."[20] As a number of scholars, officials, and commentators have also noted, a further refined and targeted version of this strategy is likely to migrate further south to the South Pacific and the strategically pivotal countries to Australia's north.[21]

From Vertical to Horizontal Networks of Power

The future of governance in the immediate region and elsewhere is uncertain. It cannot be predicted, and efforts to reconstitute it must be cognizant of complexity, as the nature of these changes is inherently discontinuous and nonlinear.[22] This disruption is driven by four interlocking characteristics of the age of digital information networks, detailed below. The ubiquity of information in the digital era has caused a diffusion of power among a diversity of actors in the international system. However, as indicated in Kilcullen's 2004 *Complex Warfighting* operating concept, while the increased diversity of actors is not a new trend, it is how these actors wield power through flattened power structures that represents a marked change.[23] In the unfolding strategic context, power no longer strictly flows through vertical hierarchical institutions upon which sits the state, but rather flows horizontally through complex networks in which the role of the state and its ability to exercise power is unclear.[24] Individuals, social groups, organizations, and state actors as distinct and indistinct entities and in side-by-side relationships are involved in the transmission of ideas and the exploitation and manipulation of information as a means to gain strategic advantage. As a number of authors attest, IW waged through these horizontal networks upsets the balance of power as its means do not favor the traditional remit of vertically hierarchical conventional militaries.[25] In the information domain, advantage is hard to achieve and maintain as "a narrative can now deploy in a rapid-fire series of mutually reinforcing stories that are hard for people to disregard and reach a global audience in seconds at minimal costs."[26] Furthermore, the rapid deployment of narratives can create chaos and undermine the rules-based global order and those that stand in support of it.[27]

China has conducted a concerted information campaign through statements of senior officials and state-owned media outlets to develop a narrative of victimization and rightful historical ownership of land features in the South China Sea.[28] This narrative is intended to foster perceptions that China's extension of power into the South China Sea is a defensive measure, and therefore the behaviors of those contesting China's actions are offensive. At the same time, little information has been released to the public from U.S. intelligence agencies regarding China's activities, further facilitating China's own narrative.[29] Operatives of the Russian Internet Research Agency, a Kremlin-associated group run by oligarch Yevgeny Prigozhin, exploited existing partisanship and disenfranchisement in the U.S. political system.[30] Their use of fake profiles on social media platforms, including but not limited to Twitter and Facebook, to spread suspicions against key political figures, namely within the Democratic Party, was a highly effective, yet unseen offensive against American democracy.[31] Before Russia, militant extremist group al Shabaab, and later the so-called Islamic State, used a wide range of social media platforms to transmit its propaganda and amplify its voice to construct a narrative of religious superiority and moral higher order to support calls for jihad.[32]

Expansion of the *Cognitive* Battlespace

Corresponding with the expansion of digital horizontal networks, the cognitive battlespace has expanded dramatically while eluding formal characterization within military and intelligence communities. The shifts in the strategic landscape suggest its time has come and a cogent definition and lexicon are now overdue. IW is an enduring feature of warfare. Early 1990s conceptualizations of IW viewed it as a component of the overall military battlespace and as a convergence of separate lines of effort that included all elements of intelligence, surveillance, and reconnaissance, electronic warfare, psychological operations, and cyber operations. However, a unity of effort under a unified theory of IW did not materialize, and the elements of IW continued to develop and evolve as more or less distinct operational efforts supplementary to kinetic effects.[33] Concepts of "cognitive warfare" were introduced but remained indistinct from the broader IW discussion within military and intelligence communities.[34] A brief overview of the cognitive battlespace and cognitive warfare is offered below.

Broadly speaking, *cognition* describes the mental process by which information is transformed into knowledge and knowledge into understanding.[35] As early discussions of IW pointed out, human understanding of the battlespace is the essence of situational awareness and the basis of strategic decisionmaking and action.[36] Contests for information assurance and security involving attempts to deny, degrade, and destroy adversary information have always occurred in a "cognitive battlespace." These efforts now include but are not exhausted by all the elements of IW mentioned, and thus involve both human and cyber systems and dissolve the civil-military divide. The point of departure is in the exploding use of computers as persuasive technologies—the set of practices termed *captology* by Stanford

U.S. troopers, assigned to A Battery, Field Artillery Squadron, 2nd Cavalry Regiment, raise assembled radio antenna to enable field communications during Operation *Chosin* at 7th Army Joint Multinational Training Command's Grafenwoehr Training Area, Germany, January 28, 2015 (U.S. Army/Gertrud Zach)

University's B.J. Fogg in 1997.[37] It is by way of the uniquely persistent, proximal, and continuous forms of contending availed by digital technologies, accessing the minds of others anonymously and from extended range, that IW efforts have merged into an expanded cognitive domain. These contests taken as a whole amount to "cognitive warfare," the sum of which is greater than its individual parts, and where the unintended side effects of intended persuasive activities are unpredictable and emergent. Effects in the cognitive battlespace have the capacity to alter the context of situational awareness, thus rendering it incomplete. Incomplete situational awareness can reflect an orientation toward information that obscures its meaning. Capabilities deployed under a false orientation cannot achieve the desired strategic effect. Worse still, the capacity to recognize and adapt to the shifting circumstances can be thwarted.

Cognitive warfare is an enduring feature of the existing and future operating environment. By connecting all domains, it blurs distinctions between war and peace and operational levels. The unification of lines of effort and effects under preexisting IW constructs has been forced on operators by a combination of the shifting strategic circumstances and by the efforts and activities of not only adversaries but also private-sector captology practices with no malignant intent, effectively creating a new terrain. The transformative impact of the weaponization of the cognitive domain extends well beyond existing conceptualizations of the problem space. In turn, the erosion and delegitimization of the liberal internationalist narrative change the context in which the United States and its allies may seek to exercise kinetic power. This terrain and its informational content connect the traditional physical domains of warfare to human systems, and there is no firewall dividing civil and military domains and no sentinel currently protecting the domestic population. Sophisticated and coordinated information operations traversing this terrain are poised to target the political, cultural, and moral centers of gravity of society, leveraging all elements of the connectivity, reach, and persistence of the medium.

No better example to date exists than the Russian manipulation of various social media platforms in the 2016 U.S. election, acknowledged on July 3, 2018, by the U.S. Select Senate Committee on Intelligence (SSCI) report, which confirmed the U.S. Intelligence Community Assessment produced in January 2017.[38] Having foreseen "the broad impact of technology on the battlespace," Russia has effectively leveraged the shift to horizontal information networks and the expansion of gray-zone warfare.[39]

While very much in its formative stages, U.S.-based military and intelligence communities have begun to develop a lexicon for cognitive war that contains analogies with elements of traditional kinetic warfare.[40] From these early conceptualizations, the concept of information effects is being refined. The advent of hyper-connectivity has added the carefully tailored narrative to the arsenal of information effects.[41] The narrative, injected into the information cycle at the critical time, can be described as a form of "cognitive fire." Cognitive fires are now precision-guided, and the kill chain is transversal. Cognitive fires emit a "narrative signature" in the electromagnetic spectrum, analogous to an aircraft wing in the radio spectrum or a combustion engine in infrared.[42] To an extent, they can be identified and tracked. However, when a weaponized narrative leaps inevitably from cyberspace into analogue physical space, its signature gets disseminated and, in many cases seen recently, its effects both intended and unintended can be exponentially magnified. This exponential payoff in effects is what defines cognitive fires as a strategic weapon of unprecedented power. The Russian information operations identified in the SSCI report benefited precisely from this payoff. The strategic ramifications, therefore, are not limited in the same way as adversaries' employment of high-tech weaponry or the cyber warfare targeting of command and control of deployed armed forces. The strategic implications extend to the vulnerable cognitive fabric of the open society from which the armed forces of liberal democracies draw the entirety of their resources.

Constant, Unrestricted, and Unbounded Warfare

As the cognitive battlespace expands, the strategic threshold, once determined as a discernible point on a linear continuum by traditional markers of conflict escalation, now transverses a multidimensional nonlinear matrix of competition and conflict. In the cognitive battlespace, lines demarcating civil and military spaces and conditions of peace and war are being blurred and reconstituted. Adversary lines of effort are increasingly aimed below a threshold at which conventional combat capabilities would be engaged. Both Russia and China have employed integrated military and nonmilitary mechanisms aimed directly at the strategic level, bypassing operational level campaigns, which extend beyond the limits of the physical battlespace.[43] Iran's constant, unrestricted, and unbounded warfare strategy leverages Hizballah to cause societal and political chaos for its adversaries.[44] This strategy, bypassing the strengths and authority of traditional militaries, is not the preserve of militaries but is open to all. As Clint Watts suggests, the concern now should be how everyone, state and nonstate, might seek to employ similar strategies and the consequences of mass chaos in a world in which the capacity to distinguish truth from fiction is in precipitous decline.[45]

This strategy is intentionally designed to play to the weaknesses of Western liberal democracies by attacking their soft underbelly.[46] Military and legal responses to adversaries' efforts that blur the line between militaries and civilian populations and acts of war debilitate liberal democratic norms and principles of international law. Effective responses must be oriented to reflect this blurring and reconstitution of the relevant battlespace.[47] The integrated incorporation of informational effects with physical effects, in both offensive and defensive contexts, can orient the armed forces toward the "cognitive main effort" they will require while defending the peace as well as to fight and win in the future operating environment. A cognitive main effort requires whole-of-government coordination and support, and will require significant organizational adjustment within the Australian Defence Organisation.[48]

Erosion of Trust in Western Liberal Democratic Institutions

The dislocation of states from their traditional hierarchies and the failure of governance are both caused by and enforce the erosion of ideas, norms, and trust upon which the Westphalian state and rules-based order are predicated. The loss of trust in centralized Western liberal democratic institutions and their ability to govern after the 2007–2008 global financial crisis is now exacerbated by the advent of peer-to-peer digital platforms, including but not limited to social media, through which ideas about the failure of Western democratic institutions and decentralized self-governance models are transmitted. Soon, distributed ledger technology, commonly known as "blockchain," will add new and novel variances to the human-computer interface as institutions such as banks, governments, and corporations seek a secure foothold out of what is widely recognized as a rogue cyber domain.[49] These and other technology-driven changes represent radical and untested interventions in analogue systems of trust.

According to the 2018 Edelman Trust Barometer, the trust that was dislocated from vertical liberal democratic institutions to digital platforms is now also in decline as the findings of the Robert Mueller investigation are made public and people come to realize that the person they correspond with via these networks may not be a "peer" but rather a bot.[50] How trust in a post-truth world will be reconstituted in horizontal networks and the role of the state within are yet to be determined.[51] At the same time, the 2018 Edelman barometer shows that trust of a different type—transactional in nature—has increased in authoritarian systems, most notably China, which now holds the number-one trust rank. Here the broader implications of proliferating disinformation activities are clear. Not only battles *for trust*, but contests *of trust*, to reorient its meaning between different political-economic systems—democratic and authoritarian—characterize this strategic contest. Leading scholars from the intelligence, military, and academic communities are recognizing this fundamental shift: "The most prominent operations of the last year—Russian attempts to undermine the 2016 American Presidential election through the hacking of the Democratic National Committee, the release of emails, and the use of fake Facebook and Twitter accounts—were designed to undermine trust in institutions through manipulation, distortion, and disruption."[52]

IBM's Watson for Cyber Security uses cognitive capabilities to improve cyber security investigations (IBM/John Mottern)

Developing Trust to Navigate Uncertainty in the Cognitive Battlespace

The future of global governance and the Western liberal democratic model is yet to be determined and may be in a state of contested reconstitution indefinitely. The interplay of social and technological trends, from which the threat to the strategic narrative and global governance model emerges, is characteristically nonlinear and therefore cannot be predicted, and plays out below a threshold in which the attention and resources required to respond are likely not forthcoming from highly distracted societies and government institutions. This is fundamentally because the interplay is occurring within complex and multifaceted human and nonhuman systems about which we as observers have inherently imperfect knowledge. The threat is by its nature an orientation challenge, driven by the complexity in the speed and scope of change. This means that the more immediate strategic problem for the Australian army is not in meeting a peer adversary on the conventional battlefield, which is a low-probability, high-impact operational and tactical scenario, but the uncertainty of governance, stability, and peace at both local and global levels in the face of contending narratives that erode the incumbent social-political settlement upon which civil peace—domestic and international—is predicated. *Relational* trust, therefore—the voluntary acceptance of a level of vulnerability in the presence of pervasive uncertainty—is a strategic resource that represents the connective tissue of Australian and allied power, and it requires acknowledgment and cultivation as a type of "immunity boost" for sociopolitical stability and sustainability, not retreat and abandonment.[53]

Trust cultivation and prioritization are active strategies to reestablish the conditions in which preferred supporting narratives can be forwarded. Without the trust component, the narrative and associated order become one of reactive self-interest and short-term transactionalism, which provides benefits to the highest bidder and the most materially endowed. Power and influence become a numbers game, one that would offer particular benefits to authoritarian adversaries. Building trust avoids succumbing to an attempt to directly counter the strategic aims of the adversary, which further erodes the fabric of open societies and works to alter the rules of the game to adversary advantage. It provides the heuristic needed to underpin the necessary unified narrative to coordinate joint and whole-of-government activities—for example, international engagement, information operations, IW, and psychological operations—in the cognitive battlespace and the means to deny the adversary strategic space gained through "information fratricide," a consequence of discordant strategic messaging. Coherence can only be achieved as a product of strategic engagement that augments and aligns existing disparate lines of effort conducted under the auspices of a cognitive main effort. Without the coherence of narrative provided by trust, the cognitive main effort succumbs to an analogue of blue-on-blue conflict, to use kinetic terms.

For an army, this requires a reorientation of its international engagement strategy as an ad hoc line of effort in support of kinetic operations. The development of relational trust requires *strategic* engagement—enduring in nature and coordinated for a unified strategic message as the U.S. Echelons Above Brigade (EAB) concept concurs. U.S. Army efforts in this regard are well advanced. U.S. Army Training and Doctrine Command Pamphlet 525-3-8, published December 6, 2018, details how the Service's EAB concept can better support operations across the "competition continuum," with particular focus on persistent competition below the threshold of armed conflict, with irregular and unconventional combatants and capabilities, and emphasizes the pervasive cognitive element,[54] as described above. It envisions persistent and continuous EAB formations and commanders as *never ceding the initiative*, being *anticipatory* rather than reactive, and remaining *skeptical* of their own understanding throughout a campaign or operation due to the inherent complexity of the contemporary battlefield.[55] Acknowledging the significant civil-military cooperation required to achieve these ambitious goals, Assad Raza and Jerritt Lynn argue that EAB formations must be complemented by a unified civil affairs regiment under the joint command of the communities of interest they represent within the armed forces, which can nonetheless carry forward the government's strategic intent. According to Raza and Lynn, the envisioned U.S. Joint Civil-Military Operations Center would serve as an

> *operational- to strategic-level organization to maintain continuous coordination with interagency partners, [which] would facilitate cooperation with interagency partners in areas of common interest, promote a common civil operational picture, and enable sharing of critical information and resources to support population-centric operations, [providing] commanders a unique capability to help resolve population-centric problems that could negatively impact military and civilian efforts.*[56]

The concept is closely aligned with the "cognitive main effort" we describe above and expressed in our recommendation for the role of strategic engagement within the Australian army.[57]

To achieve this outcome and meet strategic guidance would require a significant change in the role of the army, which would need to be articulated in the Australian army's operating concepts. Close combat capabilities will remain a cornerstone of the remit of Australian Land Forces. Modernization programs should be maintained to sustain a combat capability. At the same time, the army could expand upon elements of its traditional remit to support whole-of-government efforts to address the growing strategic vacuum that exists below the threshold of conventional armed conflict. This would involve a paradigm shift from the traditional notion of top-down military-to-military and civil-military cooperation to allow for new forms of bottom-up and side-by-side cooperation, which leverage a coherent strategic narrative to introduce a cognitive main effort to the army's remit. This requires a prioritization of strategic engagement specialists trained specifically with the appropriate skill sets within a dedicated force structure construct.[58]

This proposal represents a paradigm shift for the Australian army. Relational trust develops over time, through deepened and sustained civil-military and military-to-military interactions, from the bottom up and side by side across levels of society. Furthermore, the army's efforts to build trust as a counter to adversaries should also be directed internally within Australia, as there is no firewall dividing the narrative the army needs to project overseas and the narrative it needs to project domestically. Leveraging trust as a strategic resource requires sustained commitment and focus. It should be treated as part of the Australian army's core business rather than as "accessories that serve military requirements,"[59] or the remit of the special forces.

Here the opportunity exists for the army to lead the strategic response to develop trust between Australia and key domestic, regional, and global partners. In its ability to build trust from the bottom up and side by side, the Australian army uniquely contributes to joint and whole-of-government international engagement efforts.[60] This would offer particular benefits to the special forces, whose own unique efforts would be greatly facilitated by a more favorable operating environment. Existing strategic engagement efforts do not extend far enough and are not structured to fulfill the aim of establishing enduring relational trust-based relationships across the region and abroad. Periodic ship visits, joint exercises, capacity-building, and cultural exchanges are important but insufficient to respond to the persistent challenges of the shifting operating environment. The augmentation of the Australian army's civil-military information center capability, potentially leveraging expanded reservist forces trained with a specific skill set, could provide the scale-appropriate niche capability for the army, whether acting independently or in an alliance contingency. Enabled by its strategic agility and innovation, the army's impact will be to leverage mass through enduring strategic effect in order to realize a truly *strategic army*.

Conclusion

Rapid shifts in the future operating environment present traditional Western armies with a number of strategic risks, including the speed and scope of change in the human and technical environment, and the expression of these elements through the prism of increasingly diverse and unpredictable threats to the regional and global rules-based order. These threats have emerged from the technology-driven shift from vertical to horizontal digital information flows and the associated degree of hyper-connectivity. This results in an expanded battlefield, with an increasing emphasis on cognitive vulnerabilities that do not discern between military and civilian domains or conditions of peace and war. This gives rise to a high-tempo threat environment of constant, unrestricted, and unbounded warfare. Together, these shifts in the strategic landscape amount to what is essentially a cognitive contest, one that goes beyond existing risk modeling and challenges the army to account for broader types of threats. This challenge reveals the critical role played by trust in the constitution and understanding of the nature and character of threats and the required response. Trust can provide the "cognitive shield" in the changing operating environment.

The threat environment is forcing a reorientation on the army that is highly disruptive but also presents new opportunities. The necessary reorientation challenges the army to seriously consider its future roles and the structure and makeup of the key capabilities required to deliver the desired strategic engagement effects, integrated with close combat capabilities, in order to realize a *strategic army*. **JFQ**

Notes

[1] Daniel Maurer, *The Clash of the Trinities: A New Theoretical Analysis of the General Nature of War* (Carlisle Barracks, PA: U.S. Army War College Press, 2017), available at <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1365>.

[2] Mari Eder, "The Information Apocalypse . . . Is Already Here," *War Room*, August 22, 2018, available at <https://warroom.armywarcollege.edu/articles/information-apocalypse/>.

[3] See Carl Miller, *The Death of the Gods: The New Global Power Grab* (New York: Random House, 2018).

[4] Nathan Freier and Jonathan Dagle, "The Weaponization of Everything," *Defense One*, September 9, 2018, available at <www.defenseone.com/ideas/2018/09/weaponization-everything/151097/>; Ariel E. Levite and Jonathan Shimshoni, "The Strategic Challenge of Society-Centric Warfare," *Survival* 60, no. 6 (November 2, 2018), available at <https://doi.org/10.1080/00396338.2018.1542806>.

[5] Alicia Wanless and Michael Berk, "The Strategic Communication Ricochet: Planning Ahead for Greater Resiliency," *The Strategy Bridge*, March 7, 2018, available at <https://thestrategybridge-org.cdn.ampproject.org/c/s/thestrategybridge.org/the-bridge/2018/3/7/the-strategic-communication-ricochet-planning-ahead-for-greater-resiliency?format=amp>.

[6] Emily Bienvenue et al., "Monitoring the Effectiveness of International Engagement and the Health of Bilateral Relationships: A Trust-Based Framework," Defence Science and Technology Discussion Paper, 2017.

[7] Nathan P. Freier et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle Barracks, PA: U.S. Army War College Press, 2016), available at <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325>.

[8] Joseph S. Nye, Jr., "China's Soft and Sharp Power," *Project Syndicate* (Prague), January 4, 2018, available at <www.project-syndicate.org/commentary/china-soft-and-sharp-power-by-joseph-s—nye-2018-01>. The term *sharp power* was first introduced by the Washington-based National Endowment for Democracy. See "What to Do About China's 'Sharp Power,'" *The Economist*, December 14, 2017, available at <www.economist.com/leaders/2017/12/14/what-to-do-about-chinas-sharp-power>.

[9] Emily Bienvenue, Zac Rogers, and Sian Troath, "Trust as a Strategic Resource for the Defence of Australia," *The Cove*, October 29, 2018, available at <https://cove.army.gov.au/article/trust-strategic-resource-the-defence-australia>.

[10] David Kilcullen, "Complex Warfighting," Future Land Warfare Branch, Australian Army, 2004.

[11] Land Warfare Doctrine (LWD) 1, *The Fundamentals of Land Power* (Canberra: Australian Army, 2017).

[12] Robert Scales, "Clausewitz and World War IV," *Armed Forces Journal*, no. 48, July 1, 2006, available at <http://armedforcesjournal.com/clausewitz-and-world-war-iv/>.

[13] On the importance of narrative to strategic power, see Jill Lepore, "A New Americanism: Why a Nation Needs a National Story," *Foreign Affairs*, March/April 2019, available at <www.foreignaffairs.com/articles/united-states/2019-02-05/new-americanism-nationalism-jill-lepore>.

[14] John Gray, *False Dawn: The Delusions of Global Capitalism* (London: Granta Books, 2015); Karl Polanyi, *The Great Transformation: The Political and Economic Origins of Our Time* (Boston: Beacon Press, 2001).

[15] Nathan Freier et al., "Game On or Game Over: Hypercompetition and Military Advantage," *War Room*, May 22, 2018, available at <https://warroom.armywarcollege.edu/articles/the-new-defense-normal-nine-fundamentals-of-hypercompetition/>.

[16] For discussion of the term *cognitive warfare*, see Emily Bienvenue, Zac Rogers, and Sian Troath, "Cognitive Warfare," *The Cove*, September 19, 2018, available at <https://cove.army.gov.au/article/cognitive-warfare>; *Exploring Cognitive Warfare*, Over the Horizon Podcast 4, November 8, 2017, available at <https://othjournal.com/2017/11/08/oth-podcast-4-exploring-cognitive-warfare/>; Deric J. Holbrook, "Information-Age Warfare and Defence of the Cognitive Domain," *The Strategist*, December 13, 2018, available at <www.aspistrategist.org.au/information-age-warfare-and-defence-of-the-cognitive-domain/>; Dave Lyle, "The Cognitive Domain," Center for International Maritime Security, May 27, 2014, available at <http://cimsec.org/cognitive-domain/>; Kimberly Underwood, "Cognitive Warfare Will Be Deciding Factor in Battle," *SIGNAL*, August 15, 2017, available at <www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle>; Rand Waltzman, "Weaponization of the Information Environment: The Need for Cognitive Security," *Information Professionals Association*, January 10, 2017.

[17] For a definition of *relational trust*, see Bienvenue et al., "Monitoring the Effectiveness of International Engagement and the Health of Bilateral Relationships."

[18] Freier and Dagle, "The Weaponization of Everything."

[19] Gregory B. Poling, "Avoiding the False China-U.S. Narrative in the South China Sea," *American Journal of Chinese Studies* 23, no. 1 (July 2016).

[20] Jon Herrmann, "Nine Links in the Chain: The Weaponized Narrative, Sun Tzu, and the Essence of War," *The Strategy Bridge*, July 27, 2017, available at <https://thestrategybridge.org/the-bridge/2017/7/27/nine-links-in-the-chain-the-weaponized-narrative-sun-tzu-and-the-essence-of-war>.

[21] Winston Peters, "Shifting the Dial," speech, Lowy Institute, Sydney, March 1, 2018, available at <www.beehive.govt.nz/speech/shifting-dial>; Euan Graham, "Conserving the Single Maritime Operating Environment," speech, Exercise Kakadu Fleet Commanders Conference, Lowy Institute, September 1, 2018, available at <www.lowyinstitute.org/publications/conserving-single-maritime-operating-environment-euan-graham>; Ben Bohane, "South Pacific Nation Shrugs Off Worries on China's Influence," *New York Times*, June 14, 2018, available at <www.nytimes.com/2018/06/13/world/asia/vanuatu-china-wharf.html>; Liam Fox, "Tonga to Start Paying Back Controversial Chinese Loans Described by Some as 'Debt-Trap Diplomacy,'" ABC News, November 18, 2018, available at <www.abc.net.au/news/2018-07-19/tonga-to-start-repaying-controversial-chinese-loans/10013996>; David McCabe, "Go Deeper: Why China Hasn't Followed Russia on Disinformation—Yet," *Axios*, August 6, 2018, available at <www.axios.com/china-and-russia-online-disinformation-election-meddling-255d7196-41da-4f1b-9fdf-2f185218cb2c.html>.

[22] On the challenge to forecasting amid complexity, see Dan Gardner, *Future Babble: Why Expert Predictions Fail—And Why We Believe Them Anyway* (Toronto: McClelland & Stewart, 2010); Philip E. Tetlock, *Expert Political Judgment: How Good Is It? How Can We Know?* (Princeton: Princeton University Press, 2017); Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Random House, 2015); Nassim Nicholas Taleb, *Incerto: Fooled by Randomness, The Black Swan, The Bed of Procrustes, Antifragile* (New York: Random House, 2016).

[23] Kilcullen, "Complex Warfighting," 7–8.

[24] Anne-Marie Slaughter, "How to Succeed in the Networked World: A Grand Strategy for the Digital Age," *Foreign Affairs*, December 2016, available at <www.foreignaffairs.com/articles/world/2016-10-04/how-succeed-networked-world>.

[25] Ian Tunnicliffe and Steve Tatham, "Social Media—The Vital Ground: Can We Hold It?" Strategic Studies Institute, U.S. Army War College, April 21, 2017, available at <https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1349>; James P. Farwell and Darby J. Arakelian, "Using Information in Contemporary War," *Parameters* 46, no. 3 (Autumn 2016), 71; Gideon Avidor and Russell W. Glenn, "Information and Warfare: The Israeli Case," *Parameters* 46, no. 3 (Autumn 2016), 99; David Betz, *Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power* (Oxford: Oxford University Press, 2015).

[26] Herrmann, "Nine Links in the Chain."

[27] Ibid.

[28] "Yang Jiechi Gives Interview to State Media on the So-Called Award by the Arbitral Tribunal for the South China Sea Arbitration," Embassy of the People's Republic of China in Canada, July 15, 2016, available at <http://ca.china-embassy.org/eng/zt/cpot/t1381769.htm>; see also "China's Position on the Territorial Disputes in the South China Sea Between China and the Philippines," Embassy of the People's Republic of China in Canada, April 4, 2014, available at <http://ca.china-embassy.org/eng/zt/cpot/t1144139.htm>.

[29] Ely S. Ratner, "Exposing China's Actions in the South China Sea," Council on Foreign Relations, April 6, 2018, available at <www.cfr.org/report/exposing-chinas-actions-south-china-sea>.

[30] Adrian Chen, "What Mueller's Indictment Reveals about Russia's Internet Research Agency," *The New Yorker*, February 16, 2018,

available at <www.newyorker.com/news/news-desk/what-muellers-indictment-reveals-about-russias-internet-research-agency>.

[31] Senate Select Committee on Intelligence (SSCI), *The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections, Summary of Initial Findings*, July 3, 2018, available at <www.intelligence.senate.gov/publications/committee-findings-2017-intelligence-community-assessment>; Alina Polyakova and Spencer P. Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition," Brookings, March 2018, available at <www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf>; Malcolm Nance, *The Plot to Destroy Democracy: How Putin and His Spies Are Undermining America and Dismantling the West* (New York: Hachette Books, 2018); Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election: Unraveling the Russia Story So Far," *New York Times*, September 20, 2018; Maria Farrell, "Why Russia Is Using the Internet to Undermine Western Democracy," *Slate*, December 5, 2016, available at <www.slate.com/articles/technology/future_tense/2016/12/why_russia_is_using_the_internet_to_undermine_western_democracy.html>.

[32] Dave Lee, "The Tactics of a Russian Troll Farm," BBC News, February 16, 2018, available at <www.bbc.com/news/technology-43093390>; Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (New York: HarperCollins, 2018).

[33] Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* 11, no. 1 (Spring 2017), available at <www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf>.

[34] Peter Nicholson, "Effects-Based Strategy: Operations in the Cognitive Domain," *Security Challenges* 2, no. 1 (2006), available at <www.regionalsecurity.org.au/Resources/Files/vol2no1Nicholson.pdf>.

[35] For background on military and strategic thinking regarding cognitive processes, see Frans P.B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (New York: Routledge, 2007).

[36] Martin C. Libicki and Stuart E. Johnson, eds., *Dominant Battlespace Knowledge* (Washington, DC: NDU Press, October 1995), available at <www.dodccrp.org/files/Libicki_Dominant.pdf>.

[37] B.J. Fogg, "Captology: The Study of Computers as Persuasive Technologies," *CHI '97 Extended Abstracts on Human Factors in Computing Systems* (New York: ACM, 1997), available at <https://doi.org/10.1145/1120212.1120301>; see also B.J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do* (San Francisco: Morgan Kaufmann, 2003).

[38] SSCI, *The Intelligence Community Assessment.*

[39] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 2015).

[40] Tyler Quinn and Von Lambert, "Musings on the Prominence of Informational Effects in the Operational Art," *Grounded Curiosity*, May 21, 2018, available at <https://groundedcuriosity.com/musings-on-the-prominence-of-informational-effects-in-the-operational-art/>; Carmine Cicalese, "Redefining Information Operations," *Joint Force Quarterly* 69 (2nd Quarter 2013); Chris Telley and Scott Carpenter, "This Task Force Could Be Key to Winning in the Information Environment," *Modern War Institute at West Point*, July 19, 2018, available at <https://mwi.usma.edu/task-force-key-winning-information-environment/>.

[41] Betz, *Carnage and Connectivity*; Ajit K. Maan and Paul L. Cobaugh, *Introduction to Narrative Warfare: A Primer and Study Guide* (Eugene, OR: Narrative Strategies, LLC, June 2018); Ajit K. Maan, *Narrative Warfare* (Eugene, OR: Narrative Strategies, LLC, June 2018).

[42] Quinn and Lambert, "Musings on the Prominence of Informational Effects in the Operational Art."

[43] Wirtz, "Cyber War and Strategic Culture," 31–33.

[44] Levi Maxey, "Hezbollah Goes on the Cyber Offensive with Iran's Help," *The Cipher Brief*, January 30, 2018, available at <www.thecipherbrief.com/hezbollah-goes-cyber-offensive-irans-help>.

[45] Watts, *Messing with the Enemy.*

[46] Assad A. Raza and Jerritt A. Lynn, "The Future of Civil Affairs: Creating Regimental Order from Chaos," *Small Wars Journal*, October 2018, available at <https://smallwarsjournal.com/jrnl/art/future-civil-affairs-creating-regimental-order-chaos>.

[47] Raza and Lynn, "The Future of Civil Affairs." See also Assad A. Raza, "Great Power Competition: The Fight for Weak States," *Small Wars Journal*, January 2019, available at <https://smallwarsjournal.com/jrnl/art/great-power-competition-fight-weak-states>.

[48] Nicholas Stuart, "The New, Desperate Struggle to Secure the Critical Fabric of Society," *Sydney Morning Herald*, January 30, 2019, available at <www.smh.com.au/politics/federal/the-new-desperate-struggle-to-secure-the-critical-fabric-of-society-20190129-p50u9k.html>.

[49] Zac Rogers, "Blockchain and the State: Vehicle or Vice?" *Australian Quarterly* 89, no. 1 (January/March 2018).

[50] "Executive Summary," 2018 Annual Global Study, 2018 Edelman Trust Barometer, 2–3, available at <www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_TrustBarometer_Executive_Summary_Jan.pdf>.

[51] Zac Rogers, "Targeting Our Blind Spot of Trust: Five Impossibilities of Liberal Democracy in a Dangerous Digital Age," *The Strategy Bridge*, January 28, 2019, available at <https://thestrategybridge.org/the-bridge/2019/1/28/targeting-our-blind-spot-of-trust-five-impossibilities-of-liberal-democracy-in-a-dangerous-digital-age>.

[52] Neal A. Pollard, Adam Segal, and Matthew G. Devost, "Trust War: Dangerous Trends in Cyber Conflict," *War on the Rocks*, January 16, 2018.

[53] For discussion of the need for a heuristic to support stability and functionality amid deepening socio-technological disarray, see Jay Cassano, "It's as if Humans Are the Problem and Technology Is the Solution," *Fast Company*, January 29, 2019, available at <www.fastcompany.com/90295374/how-to-reclaim-our-humanity-in-a-world-of-machines-douglas-rushkoff-team-human>. See especially Douglas Rushkoff, *Team Human* (New York: Norton, 2019).

[54] U.S. Army Training and Doctrine Command Pamphlet 525-3-8, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025–2045* (Washington, DC: Headquarters Department of the Army, December 21, 2018), available at <https://fas.org/irp/////doddir/army/tp525-3-8.pdf>.

[55] Ibid., 17, 35.

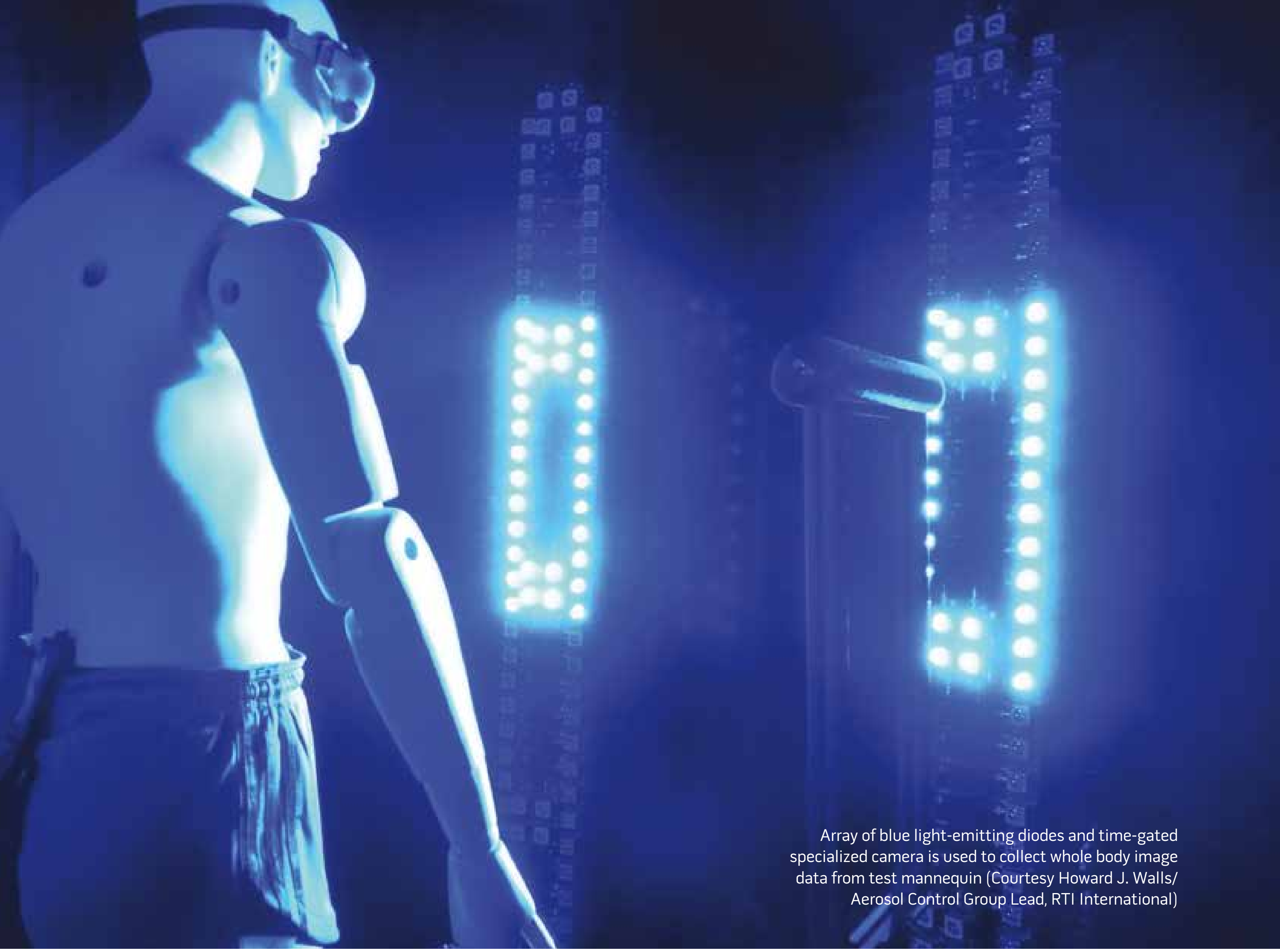
[56] Raza and Lynn, "The Future of Civil Affairs."

[57] Since 2006, civil affairs activities in support of U.S. Government objectives have been conducted under a multitude of independent and uncoordinated commands, creating organizational and strategic disfunction; see Raza and Lynn, "The Future of Civil Affairs."

[58] Greg Colton, "Defence Needs to Develop International Engagement Specialists," *The Interpreter*, December 14, 2017, available at <www.lowyinstitute.org/the-interpreter/defence-needs-develop-international-engagement-specialists>; Andrew Maher, "Strategic Planners: A Response to Operational Complexity," *Australian Army Journal* 13, no. 1 (2016).

[59] Tony Balasevicius, "Looking for Little Green Men: Understanding Russia's Employment of Hybrid Warfare," *Canadian Military Journal* 17, no. 3 (Summer 2017), 20.

[60] Rick Burr, "Army and International Engagement: Opportunities and Challenges in a Changing Strategic Environment," *The Strategist*, June 26, 2015; see also LWD 1, 8.



Array of blue light-emitting diodes and time-gated specialized camera is used to collect whole body image data from test mannequin (Courtesy Howard J. Walls/Aerosol Control Group Lead, RTI International)

Maximizing the Power of Strategic Foresight

By Amy Zalman

Dr. Amy Zalman is CEO of Prescient, a Washington, DC–based foresight consultancy. She is also an Adjunct Professor in the Culture, Communications, and Technology Program at Georgetown University.

In order to develop plans and recommend actions in support of strategic goals, national security professionals need the ability to anticipate the impacts of change in their external environment. The planner's task is complicated by the fact that from the vantage of the present, there are many possible impacts of change. In a laboratory, variables can be titrated precisely and outcomes predicted; in the national security environment, variables are dynamic and complex, and outcomes are the product of emergent interactions among people, institutions, and systems. The exact path of these interactions is inherently nonlinear and difficult to predict.

The national security strategist is thus also in need of specialized thinking skills to help him or her mentally model uncertainty and grasp the nonlinear and complex pathways of change. These thinking skills do not come naturally to the modern American military education system, which valorizes an Enlightenment-inspired scientific approach and has historically focused on teaching critical thinking skills. Such skills are valuable when a problem is well defined and it is possible to identify its component parts, evaluate evidence, and generate solutions. However, they are not sufficiently robust to address situations that are as ambiguous, loosely bounded, and complex as the possible futures of national security.

In contexts of uncertainty, another set of skills—those contained in the strategic foresight toolkit—is required. Arguably, this requirement is especially vital today: technological advancements and their unevenly distributed but powerful effects, climate change, and social change are unfolding at a challenging pace in our interconnected global system. Black swans, cascading problems, and uncertainty stemming from interconnections abound. The stakes are high for anticipating and planning effectively for the potential impacts of change.

By way of example, imagine you are a strategist in the 1970s seeking to understand the implications of the newly created Internet. Its early architects did not view Internet protocols as a potential locus of national security threat because they assumed that small communities of mutually trustworthy academics would be the most likely users of the future Internet. Critical thinking would not assist you in generating scenarios of the possible futures of the Internet, let alone conceiving of it as the foundational infrastructure of future human institutions. In open-ended situations such as the future of a new technology or institution, systems thinking and frameworks to help structure imaginative and expansive exploration of the implications of change are required. Strategic foresight supplies these frameworks.

This article makes a two-pronged argument. First, strategic foresight, a discipline I describe in more detail, provides the vitally needed mindsets and frameworks required to plan in uncertainty.[1] Strategic foresight should be taught and used more widely in the national security space. Second, where foresight is being taught and used (it has recently had an upswing in interest), there are opportunities to improve its application and better serve planning staffs and decisionmakers.

What Is Strategic Foresight?

Strategic foresight is an interdisciplinary domain that draws on cybernetics and systems thinking, management sciences, sociology, data science, cognitive psychology, and creative thinking, among others. Anticipatory thinking to support decisionmaking is its essence. The individual who invests time in learning how to think like a futurist emerges with an appreciation for the cognitive barriers faced by the human brain when it attempts to envision the future and will be well-practiced in holistic, synthetic, analytic, and creative ways of thinking. Organizations that adopt foresight practices to help them identify trends at an early stage and adapt or innovate to leverage those trends are in stronger competitive positions than those that do not. This value is demonstrable: A recently completed longitudinal study of large European firms demonstrated that those incorporating foresight into their strategic planning realized significant gains in both profit and market capitalization over the long term.[2] Management science has revealed that systematically scanning the peripheral environment for weak signals of change can help people and institutions prepare for otherwise unexpected events.[3]

Foresight is not an unknown quantity in the U.S. national security space, yet it has waxed and waned as a discipline of interest. Following sustained enthusiasm from the end of World War II through the early 1990s, interest languished as the dramatic events of the moment—the fallout from the demise of the Soviet Union, the 9/11 attacks, the 2008 financial crisis—took center stage. Recently, strategic foresight has reappeared on the radar. The growing number of conference sessions, professional education opportunities, and pursuits such as science fiction writing contests designed to trigger creative thinking about the future attest to this rise in interest. This is all good news, and, hopefully, leaders in all relevant institutions will continue to grow their support for fostering successors who are skilled at thinking both systematically and creatively about how to envision an uncertain future.

Yet enthusiastic support, while necessary, is not sufficient to create a future-minded national security workforce. It is possible to use strategic foresight well or badly. In the national security community today, there is room for improvement. Strategic foresight activities are often brought into classrooms and conference rooms in ways that are superficial. A quick exercise in scenario-building, for example, may give participants the satisfaction that they have engaged in strategic foresight. But when conducted superficially, such activities typically become exercises in *reinforcing* rather than *challenging* preexisting ideas about what the future will be like. To be clear, superficiality is never intentional. Instead, urgent pressure to produce activities leads course or activity facilitators to using frameworks and ideas that are the easiest to access instead of those that are the most appropriate. Popular ideas and activities circulate through the national security educational community uncritically, so that rough usage in one place is replicated in another, and it is difficult to get new thinking in the door.

As the history of national security community engagement with foresight demonstrates, thinking creatively about the future is a cultural challenge. Large bureaucracies, such as the Department of Defense, are often resistant to change and to reckoning with the fact that conditions for success in the future may be different from those of today. Institutional proclivities can shape and constrain the imagination that is required to develop insights into the future of a profoundly complex, changing, and uncertain world.

To take one example, futurism is frequently presented in mainstream culture as primarily associated with technological innovation. This is a narrow use of the strategic foresight skillset; technology is only one of the drivers of complex social events such as war. When they assume, rather than interrogate, a high-tech future, military participants in strategic foresight foreclose the opportunity to identify signals of change and development across the spectrum of human activity. This has in the past led to institutional blindness to signals of change in

Paratrooper assigned to Charlie Company, 1st Battalion, 508th Parachute Infantry Regiment, provides security outside subway tunnel at Fort A.P. Hill, Virginia, March 21, 2018 (U.S. Army)

societies that might produce low-tech, asymmetric approaches to armed conflict. One of the key tenets of foresight is that it is imperative to explore not only the most likely future but also a range of possible futures. It is in this arena where potential black swans lurk.

The popular premise that future wars will take place in megacities (with more than 10 million inhabitants) offers another example of how a selective use of the tools of strategic foresight can narrow strategic vision precisely where it would be useful to expand it. The war-in-megacities scenario is grounded in trend information related to the urban growth. By some accounts, there will be at least 50 such cities by 2050.[4] So it is reasonable to project that at some point, warfighters will *probably* engage in a megacity. However, strategists who halt their exploration of the future with scenarios based on the extrapolations of current trends alone are underutilizing the tools of strategic foresight. To use the foresight toolkit more comprehensively and effectively, planners will also think deeply and creatively about the *possible*, a much wider and more complex world of potential than that of simply the probable. This is not easy; it takes intellectual rigor and self-knowledge to explore trends that may violate one's institutional worldview. How could a war unfold in a nonurban area, especially in a world that is primarily urban? What assumptions are held today about what a city is and looks like? Will other emergent realities—for example, about the way people communicate and work or about how climate change and weather evolve—change the ways that cities develop in the future?

Venturing answers, however exploratory, to questions that probe beyond the boundaries of current expectations could help reduce strategic surprise in the future and prompt innovative thinking in advance of the unexpected. Strategic foresight offers compelling frameworks for asking these sorts of questions, and the frameworks themselves are not fancy or difficult to understand. This is all the more reason why advancing the understanding of strategic foresight as a discipline and a strategy support tool is not only a good idea but also a clear and simple route to creating opportunities for asking difficult questions about the potential future at a time when such questions are critical.

Strategic foresight functions best as a normal, integrated element of an organization's planning cycle. This cycle will typically include horizon scanning (also called environmental scanning) for early indicators of change, the integration of early signals into existing forecasts, impact assessments, and a decisionmaking process that uses insights of foresight to inform action.

Historically notable examples demonstrate the power of this activity. The most famous example is likely that of Royal Dutch Shell—a common tool in the foresight kit because of its pioneering use of scenarios. The oil industry historically forecast its future needs on the presumption of steadily growing demand and opportunities to locate supply. In the 1970s, Royal Dutch Shell recognized that geopolitical developments (such as the newly formed Organization of Petroleum Exporting Countries) could lead to a serious disruption in oil supply, transforming what was heretofore a buyer's market into a seller's market. As a result of its readiness to take this scenario seriously, the company was prepared for the 1973 oil embargo and recovered with greater speed than its industry peers.[5]

In the United States, the coordinated effort to prepare for potential disruptions related to the Y2K "bug" offers a powerful example of the role strategic foresight can play in raising awareness and addressing potential crises. In 1998, the World Future Society (formerly a nonprofit organization for futurists) began working with the White House, United Nations coordination groups, and others to anticipate and address potential Y2K issues in the United States. Most of their efforts were in "real-time networking and swift decisionmaking," but the group also raised awareness in a 1998 conference on the consequences that could unfold without further attention.[6] Failures of foresight are similarly dramatic, as the many well-known anecdotes of corporations and retailers that failed to recognize the potential impacts of technological and cultural trends, such as online shopping or streaming video, attest.

In the spirit of supporting this capacity, the remainder of this article offers a brief account of the role that foresight has played in military planning, followed by recommendations for advancing its implementation in military education today.

The history of foresight in the U.S. national security environment is offered here to rebut the pervasive idea among national security professionals that the United States cannot be good at long-term strategy or planning. (This idea is often justified by reference to the United States as a young country, as compared to China, a country perceived to be strong at long-term planning because it has a long history and a centrally controlled government.) This is clearly a discussion that deserves its own time and place; what can be stated here is that military futurists have played a critical role in creating some of the foundational techniques and ideas of foresight, which offer an alternative history of successful and thoughtful exploration of potential futures. It also helps to press into relief some of the cultural tendencies that might have helped planners in the past but that might be hindrances today.

Historical Snapshot

A quick survey of the history of strategic foresight as a coherent management planning discipline often begins with the example of the U.S. Air Force. After World War II, under the direction of Secretary Harold "Hap" Arnold, the Service took the first steps to connect U.S. military planning with long-term scientific and technological developments. In order to organize resources and investments, Arnold commissioned a major study titled *Toward New Horizons* that projected future technology needs for the Air Force. The planning momentum was maintained by standing up the Research and Development Corporation, known today as RAND, which became the military's go-to think tank for long-term questions and also the home of some of the country's most prominent futurists during the Cold War.

This story of foresight's foundations in the United States encapsulates the spirit of the American brand of foresight: a triumphal and empowered energy, a focus on technology as the key critical driver of future events, and a positivist outlook of the future as knowable and manageable. In the ensuing decades, this foundational vision of the postwar American future infused planning activities and also a particularly American mindset about how to think about "the future" in the abstract.

In the 1970s, the ideas of previously obscure futurists gained popularity, most notably as a result of Alvin Toffler's bestselling book, *Future Shock*. These ideas trickled into the executive offices of both government leaders and major corporations. Long-range planning and the basic tenets of foresight were accompanied by a spirit of openness and an exploratory readiness to consider the potential that more than one future might emerge. At the same time, voices of warning also called on political and military leaders to adapt U.S. planning processes to a world that was becoming more complex and interconnected. Projects such as the Department of Defense Office of Net Assessment, which was established in 1973 to assess the impact of converging macro-trends, were attuned to the need to assess complex environments.

Some of the most forceful notes of warning can be found in a 1987 volume titled *Creating Strategic Vision: Long-Range Planning for National Security*.[7] This compilation of essays outlining the various techniques of strategic foresight was offered as an antidote to the "pragmatic, fragmented, short-term" tendencies that were presumed to characterize the American way of leadership.[8] Much of this critique from a generation ago about the short-term nature of U.S. strategy has become dogma today. When I introduced the work to a cohort of flag officers in an advanced training course recently, they readily warmed to the thesis that the United States is inherently poor at long-term thinking and needs to do a better job.

Also, in the late 1980s, the U.S. Army War College introduced a new course titled Futures: Creating Strategic Visions.[9] The goal of the course was to provide promising future leaders with the creative thinking skills required to envision and communicate alternative futures in an executive setting. *Alternative futures*, in this context, refers to a practice of indicating that more than one future is possible and that one's own present-day decisions help to shape the future. The course was notable for stressing creativity as a teachable skill and for proposing that the future may unfold in many possible ways.

And there the enthusiasm stops. There is little documentary evidence in the 1990s of the creative, open-ended energy that suffused futures work in the 1980s. Indeed, the signs point in the opposite direction. The 2004 *Strategic Leadership Primer* published by the Department of Command, Leadership, and Management of the Army War College, while retaining the language of strategic vision and the future, presents the concept quite differently than it had in the 1980s.[10] Drawing grimly on President George W. Bush's 2004 remarks that the Nation's "terrorist enemies have a vision," the document calls for a countervailing one: an overarching summation of what "ought to be," subject to the ends-ways-means logic of strategy creation and capable of being summarized in a pithy image or phrase—vision, in other words, as a tagline. Little could be further from the late 1980s promotion of strategic vision as an empowering, adaptive capacity to think creatively and imagine alternative futures.

A decade later, as the mood of crisis that permeated the "hot" years of the war on terror waned, foresight activities once again emerged into national security and Federal Government consciousness. Today, we can find a Federal Foresight community of interest sharing activities across the government in the shape of formal educational opportunities, such as the Army War College futures seminar titled What Kind of Army Does the Nation Need in 2035 and Beyond; the commitment to develop an entire course on foresight at the Army Command and General Staff College; and hands-on long-term planning experiments such as the Air University's Blue Horizons program.[11] Beyond formal education, there are forums such as the periodic conferences and online community of the Mad Scientists, sponsored by the Army Training and Doctrine Command, and various think tank conferences and events. This upsurge of interest, coupled with forays in different areas of the military into more wargaming, red-teaming, and activities structured according to design theory, suggest that this is a favorable moment to advocate on behalf of not simply quantity, but also higher quality. Here are five recommendations for its achievement.

Five Recommendations to Maximize the Benefits of Foresight

Embrace Analytic Holism. The U.S. military typically privileges technological innovations as the key driver of the future, which reflects a deeply embedded tendency in American culture and history. This is problematic in several directions, all of which distort the ability to accurately assess the evidence about potential contexts of future conflict.

First, technological change does not take place in a vacuum, but at the intersection of other human institutions and drivers of change. While there is a need for pure technological forecasting in weapons development and other related areas, this work will not generate scenarios of potential future conflict. It will only produce scenarios of future weapons systems and other related technologies.

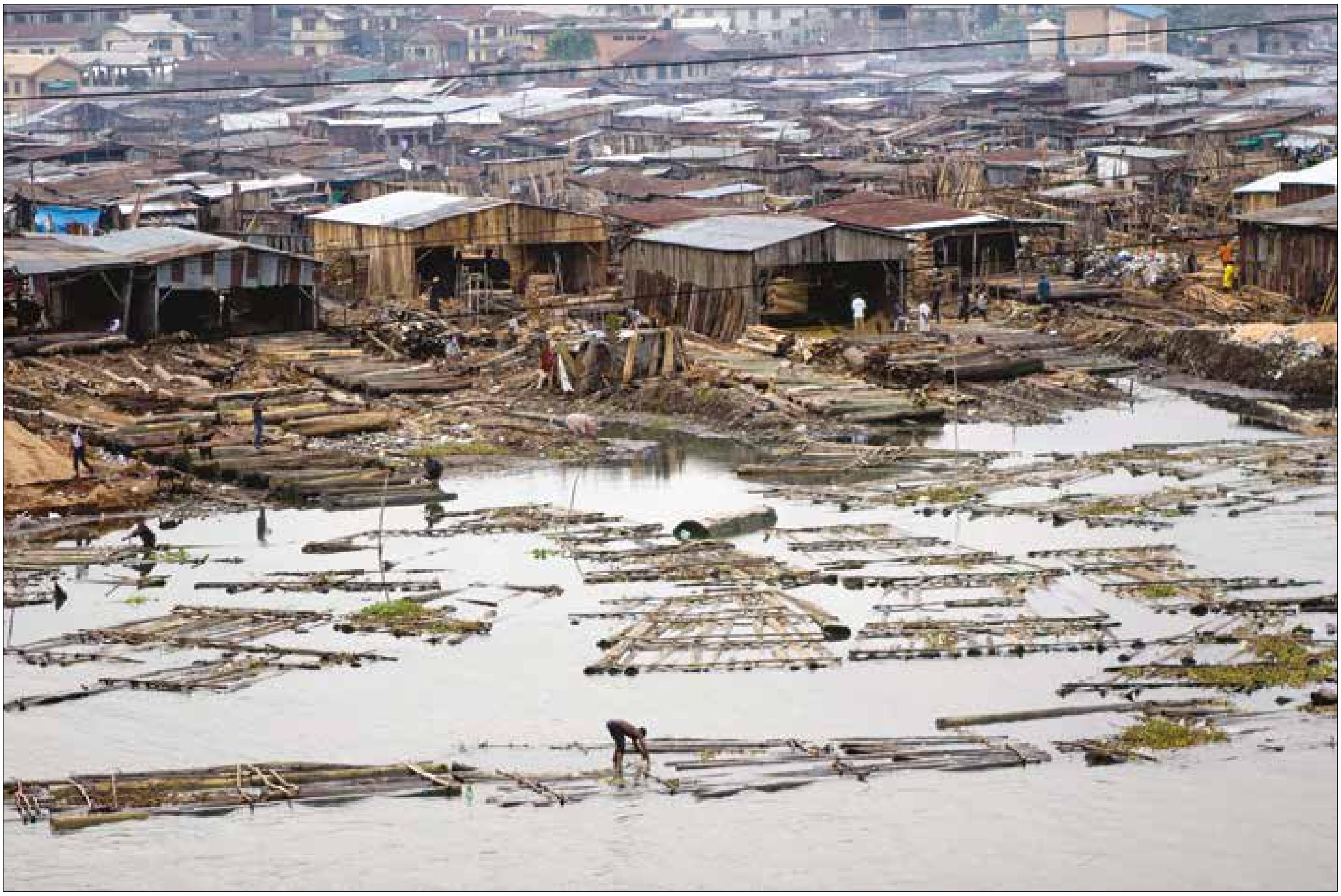
Analytic holism is a concise directive reminding participants in futures work to keep a wide range of drivers of change in mind. A traditional place to start is with the drivers encapsulated in the acronym STEEP—society, technology, environment, economics, politics. There are others, of course: cultures, demographics, media, and legal systems, to take a few obvious examples.

Change in a complex, open system, such as the international system, will occur at the intersection of developments in these areas. War and conflict, as quintessentially social events, are always shaped by developments in these areas, even when technology on the battlefield is of the essence. If planners do not look at their surrounding environment as holistically as they possibly can, they risk not seeing or recognizing signals that are eminently available for analysis and thus losing the opportunity to consider how to avoid being surprised by them. One sobering example from this century should be the social media sophistication of the planners of the al Qaeda attacks in 2001. If the national security community had been better prepared to see how, in the 1980s and 1990s, satellite television and the advent of the Internet affected social interactions around the world, it could have reduced the unwarranted surprise that "low-tech" cultures could use new media in sophisticated ways.

An even more sophisticated step in this arena will be for strategic foresight projects to start acknowledging the fundamental transformations in the global economic, political, and social systems being wrought by the ongoing evolution of digital technologies. As many commentators have noted, all of humanity is in the first stages of a new era grounded in digital infrastructure.[12] When technological innovations on this scale become ubiquitous and accepted, they actually become *less* notable in themselves as features of our world. Take, for example, electricity. Although not everyone has electricity, its ubiquity is a critical explanandum of human behavior. The world is on the way to a digital ubiquity (even though not everyone will have access to digital tools), and it is at the point of ubiquity that nontechnological drivers of change become vitally important to explore in order to posit potential future environments.

Rather than highlighting technological drivers of change and treating other drivers as "soft" or less real, strategic foresight project leaders should frame explorations of the future holistically and with a strong eye to ways in which people, collectively and individually, drive emergent and unexpected system behavior. This nuanced approach can improve the accuracy of insights into potential futures and potential surprises, even in high-tech battle space environments.

Adopt a Shared Lexicon Across the Government. Foresight terminology can be confusing. Not only does it present a number of terms of art that are also present in our everyday language (such as *foresight*, *uncertainty*, and *prediction*), but there also are differences among futurists and other disciplines in the ways they use these same words. While I might use the word *predict* in a loose and general sense to indicate my effort to explain my subjectively developed insights into how the future might unfold ("Here's how I predict the long-term impacts of negotiations over the Arctic on both trade and culture," for example), many practitioners in the strategic foresight community use



Demographers project that more than 70 percent of world's population will live in cities, many of them coastal, by 2050, and that potential for instability and strife caused by humanitarian or other disasters in megacities makes it necessary to look at them as potential future battlegrounds, Lagos, Nigeria, June 23, 2011 (Wikipedia)

the concept of prediction to refer to the narrow capacity to identify *exactly* what will happen, to a degree that is typically available only under strictly controlled experimental conditions. To add to this difficulty, many terms are somewhat similar in everyday usage ("forecasting the weather" and "predicting the weather" point to the same general idea for most purposes). Similar lexical and conceptual confusion abounds in the national security community and between different projects.

A clear and relatively simple route to orienting defense practitioners around foresight work will be by developing an authoritative lexicon and educating people across the government to use it as a reference. Other dictionaries of terms have been created—most notably by the government of Singapore, whose civil service does use the lexicon—and these and many other resources are available on the Internet for anyone's reference.[13] However, as a glance at the Singapore lexicon shows, such dictionaries are reflections of the context and priorities of their governments. A U.S. lexicon may share terminology as it is used by futurists around the world, but it will be a more authoritative resource for American professionals if it is composed with the United States in mind. Such a project will engender other benefits as well; it will create a clear point of reference for developing institutional knowledge across Services and agencies and, simplest of all, the introduction of conceptual clarity into the disparate activities by different actors.

"Get on the Balcony." The title of this recommendation borrows from the advice offered in the 1990s by management strategists Ronald Heifetz and Donald Laurie to corporations facing emerging business conditions requiring novel forms of behavior and new ways of defining and achieving success.[14] Heifetz and Laurie suggest that rather than offering solutions in such situations, leaders should galvanize adaptation to these new conditions by safely exposing employees to the challenges facing them and supporting the development of new behavioral models.

To this end, Heifetz and Laurie encouraged leaders to learn not only to view their organizations from the "field of play," where they are a part of the day-to-day work of their team, but also to "get on the balcony." From the rafters, high above the game itself, leaders can see not only competitors and the dynamics of doing business side by side with their colleagues but also the larger dynamics of the system—how different parts of the organization work together, and how they interact and intersect with the world beyond. Observations made from the balcony can provide powerful insights into the dynamics of the wider system and

From left, August Cole, co-author of *Ghost Fleet*, Chuck Gannon, author of *Trial by Fire*, and Max Brooks, author of *World War Z*, talk with select group of burgeoning science fiction writers from across Department of Defense, February 4, 2019 (DOD/Kyle Olson)

introduce opportunities to find "leverage points . . . to intervene" in the system, as the esteemed systems thinker Donella Meadows characterized the opportunity.[15] Strategic foresight education and activities offer an appropriate venue for this exploratory way of seeing the world. First, holistic vision and systems thinking are intrinsic to foresight; only by seeking signals of potential change throughout the system, and beyond one's typical domain, will one find the potential surprises and opportunities that offer competitive advantage.

This recommendation is especially salient for leaders in the U.S. national security community seeking to grapple with how to influence future events in the emerging and not yet fully understood geopolitical circumstances of the 21st century and beyond. In a rough analogy to the sports teams that serve as models for adaptive leadership in Heifetz and Laurie's work, institutions whose work is national defense tend to the see the world in terms of opposing teams. This is reasonable; it is their job. The field of play is the space from which members of the institution seek to see threats and potential adversaries.

When the world and national situations are in flux, however, this view will not provide a sufficiently comprehensive view of the evolving system—in this case, the global geopolitical, economic, and social systems. Leaders who can "get on the balcony" to view the larger context of change will see the system from an unusual vantage point that highlights flows, connections, and feedback loops not only beyond but also between parts of the U.S. defense establishment and other actors, whether these are militaries, corporations, global nonprofits, or any of the other institutional actors who make up the world.

Incorporate Complexity Thinking into Foresight Activities. Foresight and the study of complex systems arose from similar and even intertwined conceptual movements in the 20th century, and both futurists and complexity scientists draw inspiration from some of the same people—for example, Jay Forrester and Donella Meadows (and others), whose research used computer modeling in the 1970s to explore the intricate relationships between such large-scale systems as human societies and the planet's ecological systems. The interdisciplinary science that emerged in the late 1970s recognized that some systems cannot be reduced to their component parts but rather are the result of small, simple actions whose interactions can produce intricate collective behavior of the systems as a whole.

Despite these early connections with foresight, the potential contributions of complexity thinking to more effective foresight work are too often given short shrift in contemporary education and activities in the defense context. The technical specificity of terminology used by complexity thinkers, such as *complexity* and *uncertainty*, are instead reduced to brisk contextual commentary that is presented as self-evident: the world is more complex and uncertain than in the past. Once past these observations, military foresight classes and seminars typically return to the comfortably reductionist space of a future battlefield projected as more or less walled off from the other systems with which it interacts. This means that the fullest spectrum of potential scenarios that could be explored as elements of future conflict is left unexplored, since war, as a social institution, resides and interacts with other systems.

Incorporating instruction in complexity thinking could produce nuanced scenarios of possible futures and therefore result in higher quality planning. While this is not the place to elaborate in depth on complexity thinking and complex systems, we can note that a deep dive into the conceptual lexicon of complex systems, applied to the global system, can help strategists and planners to visualize the potential actions of militaries (as systems), as the porous systems they are, and to map their interactions both in and out of wars in relation to these systems. Such an activity in the runup to the second Gulf War would have usefully mapped the potential interactions of the military, industrial, national, and social systems that could be expected to interact in the case of a war.

Start Early to Build a Culture of Adaptive Leaders. This recommendation could not be simpler. Foresight mindsets and tools are too important to leave until the last moment, when a Servicemember or civilian equivalent has already become a flag officer, which is when many are first exposed to them. Foresight, in one sense, is a habit of mind, a way of seeing the world in such a way that we question our assumptions, view events holistically, and seek out the interconnections between them. These are all the kinds of habits of mind required to be the adaptive, agile thinkers who will be needed in the future. Developing an educational "ladder" that begins with habits of mind that prepare emerging leaders to think like futurists, and that continue to advanced opportunities to apply thinking skills to the open-ended challenges of the future, has the potential to advance the overall strategic capacity of the military.

There could not be a more auspicious time to institutionalize more deliberate, speculative, and imaginative approaches to thinking about potential futures of violent conflict and its management, prevention, and resolution. The world appears to be at a pivotal moment, and the need for excellent leadership on the world stage is strong. Societies worldwide are just beginning to experience the transformational effects of the shift from an industrial to a digital world and are as dramatically on the brink of the potent effects of climate change, demographic shifts, and cultural swings. There can be little doubt that emerging environments producing social stress, violent conflict, or significant displacement will have novel characteristics and the potential to look quite different from those for which the military typically prepares. In light of the acknowledged need for an increasingly adaptive and future-focused force, it is important to encourage the burgeoning interest in the future. Yet *how* this future focus is encouraged and what activities are undertaken to explore it are just as important. In this realm, there is currently room for more reflection and improvement. JFQ

Notes

[1] *Strategic foresight* has many names. It is also referred to as *futures work*, *futures studies*, *futurism*, and simply *foresight*. Several of these terms will be used within this article.

[2] René Rohrbeck and Menes Etingue Kum, "Corporate Foresight and Its Impact on Firm Performance: A Longitudinal Analysis," *Technological Forecasting and Social Change* 129 (2018), 105–116, available at <www.sciencedirect.com/science/article/pii/S0040162517302287?via%3Dihub>.

[3] George Day and Paul J.H. Schoemaker, "Scanning the Periphery," *Harvard Business Review* (November 2005), 135–148.

[4] Daniel Hoornweg and Kevin Pope, *Socioeconomic Pathways and Regional Distribution of the World's 101 Largest Cities*, Working Paper No. 4 (Toronto: Global Cities Institute, 2014), available at <http://docs.wixstatic.com/ugd/672989_62cfa13ec4ba47788f78ad660489a2fa.pdf>.

[5] See Pierre Wack, "Scenarios: Uncharted Waters Ahead," *Harvard Business Review* (September–October 1985), 73–89.

[6] Author correspondence with Kenneth Hunter, former member of the board of directors, World Future Society, May 12, 2015. Also see Jeff Minerd, "Y2K: Scenarios and Strategies," *The Futurist* 33 (April 1999), 34–37.

[7] Perry M. Smith et al., *Creating Strategic Vision: Long-Range Planning for National Security* (Washington, DC: NDU Press, 1987).

[8] Newt Gingrich, "Introduction," in Smith, *Creating Strategic Vision*, xvii.

[9] The course is fully described by its instructor, Charles W. Taylor, in his report *Creating Strategic Visions* (Carlisle Barracks, PA: Strategic Studies Institute, 1990).

[10] Stephen A. Shambach, ed., *Strategic Leadership Primer*, 2nd ed. (Carlisle Barracks, PA: Department of Command, Leadership, and Management, U.S. Army War College, 2004).

[11] For the purposes of full disclosure, I am one of the directors of the course at the Army Command and General Staff College. Separately, the activities of the Federal Foresight community of interest is available at <https://ffcoi.org>.

[12] See, for example, Kevin Kelly, *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future* (New York: Penguin, 2017); or Klaus Schwab, *The Fourth Industrial Revolution* (New York: Currency Books, 2017).

[13] *Foresight: A Glossary* (Singapore: Centre for Strategic Futures and Civil Service College, n.d.), available at <www.csf.gov.sg/docs/default-source/default-document-library/csf-csc_foresight—a-glossary.pdf>.

[14] Ronald Heifetz and Donald Laurie, "The Work of Leadership," *Harvard Business Review* (January–February 1997), 124–134.

[15] Donella Meadows, *Leverage Points: Places to Intervene in the System* (Hartford, VT: Sustainability Institute, 1999), available at <http://donellameadows.org/wp-content/userfiles/Leverage_Points.pdf>.

Interim Armored Vehicle "Stryker" and AH-64 Apache helicopters with Battle Group Poland move to secure area during lethality demonstration at Bemowo Piskie Training Area, Poland, June 15, 2018, as part of Saber Strike 18 (U.S. Army/Hubert D. Delany)

Strengthening Mission Assurance Against Emerging Threats

Critical Gaps and Opportunities for Progress

By Paul N. Stockton with John P. Paczkowski

U.S. combatant commanders (CCDRs) face an intensifying and deeply asymmetric challenge to carrying out their operational plans (OPLANs). To help execute these plans, Department of Defense (DOD) facilities and functions require electric power and other infrastructure support, typically provided by U.S. civilian-owned utilities (or host-nation assets for installations abroad). Disrupting or destroying that infrastructure offers adversaries an indirect but potentially devastating means to degrade the deployment, operation, and—ultimately—the lethality of U.S. combat forces.

Since publication of the DOD *Mission Assurance Strategy* in 2012, the Department has taken far-reaching measures to strengthen mission assurance (MA).[1] In particular, DOD has expanded its traditional emphasis on defense critical infrastructure protection and is adopting a more holistic and integrated approach

Dr. Paul N. Stockton is Managing Director of Sonecon, LLC. From 2009 to 2013, Dr. Stockton served as Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. Colonel John P. Paczkowski, USMCR (Ret.), is Senior Managing Director at Witt O'Brien's.

to support OPLAN execution by regional and functional combatant commands (CCMDs). DOD is also improving the resilience of critical nodes for defense functions and advancing new partnership initiatives with private-sector infrastructure owners and operators.

However, potential adversaries are refining increasingly sophisticated cyber weapons to disrupt and destroy industrial control systems and other key enablers of the electric grid, water systems, ports, and other support functions. Private-sector infrastructure owners and operators are also increasingly concerned that adversaries will combine cyber attacks with information warfare and kinetic strikes against key system nodes. Moreover, for installations abroad that rely on host nation–supplied energy, or on infrastructure owned and operated by Russian and Chinese companies, a simple flip of the switch could jeopardize mission execution.

DOD should counter these intensifying threats by intensifying the MA focus on supporting OPLAN execution. Exercises that assess how disruptions in U.S. infrastructure might affect the flow of forces, logistical support, and other components of such plans can help identify opportunities to strengthen MA and help DOD move beyond outdated debates over investing in "tooth versus tail." The Department should also bring cybersecurity into the heart of mission assurance and intensify the DOD focus on managing the risks posed by wide-area, long-duration power outages. However, MA initiatives should also account for the danger that adversaries will strike energy systems with both cyber and physical attacks. Moreover, adversaries could attack multiple sectors simultaneously and intensify the cascading failures between them.

Mission Assurance: Basic Goals and Ongoing Progress

The 2018 National Defense Strategy emphasizes that "the *homeland is no longer a sanctuary*." It also notes that "during conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated."[2] Especially significant, adversaries may strike the infrastructure that DOD relies on to carry out its mission essential functions (MEFs) and undermine the lethality of the joint force.[3]

Mission Assurance Strategy provides the foundation to meet these challenges. The strategy highlights how adversaries can seek "asymmetric means to cripple our force projection warfighting, and sustainment capabilities by targeting critical defense and supporting civilian capabilities and assets." The strategy also offers overarching guidance to strengthen mission assurance—that is, by building "a comprehensive and integrative framework to assess and address risks" to MEFs and using that framework to help "prioritize investments to ensure MEF performance in a constrained fiscal environment."[4]

The issuance of DOD Directive 3020.40, *Mission Assurance*, in November 2016 marked a major step forward in implementing that vision. The directive remedies a key gap in the 2012 strategy by integrating cybersecurity issues into mission assurance. The directive also strengthens DOD-wide governance and coordination mechanisms for mission assurance. Especially valuable, the document directs DOD components to prioritize MA efforts to help fulfill critical DOD strategic missions, including CCDR execution of OPLANs.[5]

DOD components are also accelerating their efforts to strengthen mission assurance. The military departments, Joint Staff, CCMDs, and other components are refining their own plans and risk mitigation strategies for MA. Moreover, they are increasing collaboration across the Department to develop holistic approaches to support CCMD OPLAN execution. However, threats to mission assurance are becoming more severe and increasingly diverse. Understanding these threats and the asymmetric strategies that leverage them is essential for assessing potential gaps in MA plans and capabilities and for developing initiatives to address these shortfalls.

Emerging Threats to Mission Assurance

The most rapidly intensifying challenges to mission assurance stem from the risk of cyber attacks on the electric power grid, transportation systems, and other civilian-owned infrastructure that defense operations depend on. This section also examines the risk that adversaries will combine cyber attacks with targeted kinetic strikes and information operations to cripple the restoration of electric power and other defense-critical services.

Cyber Attacks on the Grid and Other Supporting Infrastructure. Former U.S. Director of National Intelligence Dan Coats warned that "today, the digital infrastructure that serves this country is literally under attack."[6] Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on both civilian and government systems, including DOD. These campaigns can enable adversaries to maintain a covert presence on infrastructure networks, secrete malware designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.[7] To frame such efforts more bluntly, adversaries are *preparing the battlefield* to create massive blackouts and other interruptions of critical services whenever they deem the moment right.

Adversaries recognize the foundational importance of grid-provided power for mission assurance and will target U.S. electric companies accordingly. Cyber attacks on the grid in Ukraine in 2015 and 2016 demonstrated key threat vectors that might be employed against U.S. utilities. In these cyber-induced blackouts, attackers crossed a key threshold: they moved cyberwarfare against electric systems from theory to (limited, but still unprecedented) practice. In 2015, attackers hijacked the grid's own operating systems to disconnect critical substations, creating brief but wide-area outages. Attackers were also able to "brick"[8] operating system components and communications devices.[9]

The 2016 event displayed even more sophisticated capabilities. After mapping the grid's operating systems, attackers used the system's own incident command system (ICS) protocols to open circuit breakers, creating blackouts.[10] The malware was unusually difficult to detect and included a wiper module that could brick grid control system components on a large scale.[11] Attackers also had the ability to deny or corrupt situational awareness data, making the grid extremely prone to cascading failures.[12]

Potential adversaries are conducting "test drives" of additional ways to attack the grid and other critical infrastructure that defense installations depend on. The Dragonfly campaign, which is still ongoing today, enables adversaries to use utility vendors and other trusted third parties to conduct attacks on targeted systems.[13] Triton malware (in use since at least September 2017) enables adversaries to corrupt the safety systems that monitor and protect the performance of key system components, creating new pathways for adversaries to sabotage and intentionally mis-operate critical infrastructure.[14] Most recently, the Department of Homeland Security (DHS) reported that Russian cyber campaigns have granted them access to utility human-machine interfaces and information on accessing ICS systems.[15] Adversaries can use these interfaces—and potentially ICS systems—to shut down or mis-operate portions of the grid.

These demonstrated adversary capabilities fail to represent the true scale and severity of the threat confronting the U.S. grid and the MEFs that depend on the flow of grid-provided power. Russia, China, North Korea, and other potential adversaries have powerful incentives to hold their most destructive cyber weapons in reserve; doing so helps hobble U.S. efforts at building protections against such weapons.

Recent studies by the Department of Energy (DOE), other governmental departments, and cyber experts in academia and the private sector highlight a range of potential cyber threats that these adversaries might use to cause outages far more severe than in Ukraine. Most concerning is the potential for adversaries to compromise operator workstations or use native ICS communication protocols to intentionally mis-operate grid components.[16] Adversaries could also significantly magnify the effect of cyber-induced outages by disabling the protection systems in place to safeguard the integrity of the grid; corrupting or denying state estimation and situational awareness capabilities; and wiping, overloading, or holding "ransom" critical components or systems.[17] In the future, adversaries that employ artificial intelligence to assist their attacks will increase the potential for damage and make defense against such strikes increasingly difficult.[18]

Implications for Mission Assurance Initiatives. The severity of cyber threats to the power grid and electricity-dependent infrastructure has far-reaching implications for MA policies and programs. Indeed, given the dependence of DOD force projection on civilian-operated ports, transportation assets, and other infrastructure, accelerating the restoration of grid-provided power will be of prime importance for mission assurance. This dependence on private infrastructure is not new. The U.S. military has long relied on civilian transportation and communications systems for operational logistics. However, adversaries are increasingly threatening this infrastructure as a means to disrupt and degrade U.S. warfighting capabilities. Building resilience against these threats will require new and deeper levels of collaboration with grid owners and operators.

One especially valuable focus of collaboration has been to improve the ability of defense installations to execute MEFs with emergency power. A growing number of defense installations are becoming capable of operating as "power islands," separated from the surrounding grid and able to serve critical loads with emergency generators, on-site fuel, and electricity distribution systems. These improvements are vital and must be sustained.

Emergency power capabilities, however, will be at increasing risk if adversaries create wide-area, long-duration power outages. In blackouts lasting more than a week, emergency power generators will start breaking down, and fuel resupply could become increasingly difficult to sustain. Moreover, many defense installations rely on grid-dependent infrastructure outside their perimeters (and beyond the reach of their emergency power systems). Installation personnel typically live in and commute from communities surrounding their bases. Water and wastewater systems, regional hospitals, and other supporting infrastructure that these personnel depend on will fail in long-duration outages. These disruptive effects will also cripple port operations and contractor-provided logistical systems essential to deploying and sustaining U.S. combat forces abroad. DOD MA initiatives should account for these risks and develop holistic strategies to support OPLAN execution.

Combined Cyber-Physical Threats and Additional Risks to Critical Infrastructure. Physical attacks on the grid add another threat vector for mission assurance. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

Electrical industry leaders have been increasingly concerned about the disruptive potential of kinetic attacks on grid infrastructure since the physical attacks on the Metcalf substation in April 2013. Fortunately, an adversary would face greater risks when launching physical rather than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck. Yet the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone.

Unmanned aerial vehicles (UAVs) could also pose increasingly complex

First Security Forces Assistance Brigade Soldier uses Drone Defender with electromagnetic pulse to disable, capture, and control target drone, Camp Buehring, Kuwait, March 6, 2018 (U.S. Army/Brent Thacker)

kinetic threats. Improvements in drone technology and low-cost options increase the potential for adversaries to use UAVs to attack U.S. infrastructure, especially if they are equipped with improvised electromagnetic interference devices or other advanced payloads.[19] Even relatively simple UAVs can defeat traditional physical protections that focus on deterring or stopping armed personnel. Long-range drones could also present particular challenges for facilities overseas around which the United States does not control the airspace.

Even more concerning, however, is the threat that adversaries may launch combined cyber-kinetic attacks. The premier exercise system for the North American power grid, the GridEx series, is built around such combined threats because they could create multiweek power outages over multiple areas of the United States.[20] In particular, if adversaries can use physical attacks to destroy transformers and other critical electric infrastructure, and/or (potentially) deploy active shooters against utility employees once the attack is under way, the difficulty of defending the grid will be significantly greater than against cyber weapons alone.[21]

Electromagnetic pulse (EMP) attacks present another potentially catastrophic attack vector. The electric industry and its Federal partners are already strengthening preparedness against EMP attacks. For decades, DOD has taken measures to ensure the survivability of key communications systems and other defense assets against EMP threats. DOE and DHS have launched initiatives to help grid owners and operators protect their own systems against EMP effects.[22] Until recently, however, DOD has provided little support to electric utilities on hardening technologies and other protective measures, even though the disruption of power supplies in an EMP attack could significantly degrade the ability of defense installations to execute their MEFs.

Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. GridEx employs a threat scenario that includes combined cyber-kinetic attacks on power companies in multiple U.S. regions, as well as adversary information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past U.S. power outages. These disinformation operations could complicate efforts to provide defense support to civil authorities. They could also magnify the difficulty of ensuring that civilian employees for ports and other infrastructure

During loss of commercial power to Incirlik Air Base, Turkey, Airmen from 39th Logistics Readiness Squadron receive fuel from bladder off C-5M Super Galaxy, July 22, 2016 (U.S. Air Force/Caleb Pierce)

essential to MA continue to perform their functions.

Cross-Sector Interdependencies: A New Frontier for Mission Assurance. U.S. critical infrastructure sectors are becoming increasingly interdependent. These cross-sector dependencies are creating new risks of infrastructure failure and significant opportunities for adversaries to magnify the effects of their attacks on the power grid and other systems essential for MA. Accounting for this shift in the architecture of U.S. infrastructure will be essential for supporting OPLAN execution by U.S. defense installations.

The most immediate cross-sector risks to mission assurance lie in the interdependencies between natural gas transmission systems and the electric grid. A growing number of proposed DOD microgrids will rely on natural gas to fuel their generators. Moreover, in California, New England, and many other regions of the United States, gas provides an increasingly dominant source of fuel for generating grid-provided electricity for defense installations.

As natural gas has become an increasingly important fuel for electric generation, natural gas pipelines have also come to rely on electricity to function. Key components of gas pipeline systems, including the compressors and industrial control systems that keep gas flowing to power generators and other users, are more reliant on electric power. Adversary-induced outages could interrupt the flow of electricity to these components and (in a classic case of spiraling effects) magnify those outages by disrupting gas deliveries to power generators essential for power restoration.

MA initiatives will need to account for the risks created by these and other infrastructure interdependencies. It would be dangerously shortsighted to assume that gas-fired generators for DOD microgrids provide resilient power, without also ensuring the resilience of the natural gas pipelines that provide fuel for these generators. However, the potential for mutually reinforcing failures is not unique to the oil and natural gas subsector, and failures in other sectors could also threaten mission assurance. Equivalent challenges will exist for managing the risks posed by interdependencies between the grid and water systems, communications systems, and other tightly coupled infrastructure sectors. Public-private partnerships (P3s) focused on the electric industry and other sectors are necessary but not sufficient; to strengthen mission assurance, DOD will also need to conduct multisector risk analyses and mitigation initiatives.

Mission Assurance Abroad. For many CCDRs, especially in regional commands, executing OPLANs will require support from bases outside of the continental United States (OCONUS). Major U.S. bases in Europe, the Far East, and other areas depend on the same infrastructure services as installations in the United States. In particular, these bases depend on host-nation power grids to function (though they also typically have emergency power capabilities). Utilizing grid-provided power in OCONUS installations can significantly reduce energy costs. A comprehensive assessment of OCONUS base power options found that "in every case, it was found that bases connected properly to host nation power grids . . . would reduce the cost of energy for those bases, reduce fuel usage (and the associated logistic challenges), and increase base endurance. This was true even in cases where the host nation power grid had very low reliability." Accordingly, the study "strongly recommended that every U.S. military base consider using host nation power."[23]

Dependence on host-nation infrastructure services, however, carries significant risks. The July 2016 cutoff of power to a U.S. Air Force air base in Incirlik, Turkey, exemplifies these risks. Incirlik Air Base is essential for conducting U.S. military operations against the so-called Islamic State (IS), using manned and unmanned aircraft. The Turkish government cut off commercial electric power to Incirlik for nearly a week in 2016, following a failed coup attempt by members of the Turkish armed forces. A recent study of the event found that while the air base made use of standby generators, the Air Force was forced to reduce the number of sorties flown. Had the power outage continued, the Air Force would have had to stop flying altogether.[24] The bottom line: host nations can jeopardize mission assurance and OPLAN execution with a flip of the switch.

The foreign-owned infrastructure on which OCONUS installations depend is also vulnerable to the same cyber and kinetic threats that confront U.S. infrastructure. In Japan, for example, cyber threats from China, North Korea, and other potential adversaries are intensifying at least as rapidly as against the United States. However, Japan has been slower to buttress its cyber resilience.[25] Strengthening emergency power capabilities on U.S. installations will be essential to mitigate the risks of cyber attacks on host-nation infrastructure. DOD should also explore partnership opportunities to help strengthen the resilience of allied power grids.

Infrastructure interdependencies create additional challenges to U.S. mission assurance abroad. For U.S. installations in Europe, the dependence of local power generation on Russian-supplied natural gas provides a special threat. The Nord Stream-2 gas pipeline project will increase the leverage of Russia's Gazprom, which currently supplies around one-third of European Union gas. In 2009, Russia cut off gas supplies to Ukraine, with downstream consequences for the European Union. Amos J. Hochstein, U.S. Special Envoy and Coordinator for International Affairs, emphasizes that "our commitment to energy security in Europe is directly linked to our concern for national security."[26] That commitment must extend to strengthening mission assurance for U.S. installations reliant on Gazprom-fueled electricity generation.

Finally, China and other potential adversaries are buying up (and helping to operate) infrastructure around the globe, including in nations where U.S. defense installations support OPLAN execution. Chinese companies are rapidly increasing their investments in and ownership of foreign power and gas networks, buying assets in the United Kingdom, Spain, Australia, and Latin America.[27] These ownership and operation trends create an additional threat vector to manage and reinforce the need to bring OCONUS installations into the core of future mission assurance initiatives.

Recommendations

DOD is taking major steps to combat all the threats examined above. The analysis that follows offers recommendations on how DOD can ramp up that progress and expand the partnerships necessary to strengthen mission assurance.

Shifting the Paradigm: Mission Assurance as a Component of Warfighting. DOD Directive 3020.40 established an important policy shift by directing components to prioritize the CCMD execution of OPLANs. Focusing on OPLAN execution offers a range of potential benefits. By disaggregating OPLANs and identifying specific dependencies on installations, support functions, and the infrastructure that they rely on, DOD will be able to prioritize and target resilience initiatives in ways that produce the greatest value for deterrence and warfighting. Bolstering the resilience of Defense Critical Assets and other key components of well-established Defense Critical Infrastructure Protection (DCIP) programs will remain vital. However, additional measures will be necessary against adversaries who seek asymmetric means to degrade U.S. warfighting capabilities.

The Defense Department should move beyond outdated "tooth versus tail" debates over how to invest scarce resources and adopt a risk management approach to bolster end-to-end improvements in joint force lethality. In the past, DOD invested relatively little in ensuring the survivability of supporting infrastructure. That low priority made sense at the time; DOD could conduct warfighting abroad operations without concerns that adversaries would disrupt U.S. installations and the privately owned infrastructure systems that they depended on. In recent years, however, military bases in the United States have taken on increasingly important roles in conducting UAV operations and other warfighting and sustainment activities to execute CCMD OPLANs. As DOD dependence on U.S.-based installations has grown, adversaries have ramped up their ability to disrupt the flow of power and other critical infrastructure services that those bases rely on. Intelligent, adaptive adversaries will seek to defeat the United States without facing the point of its spear. Treating infrastructure resilience as a core warfighting requirement, and ensuring that adversaries cannot break the shaft of that spear, constitute an essential paradigm shift for mission assurance.

DOD should also intensify the focus of MA on supporting the execution of CCMD OPLANs. Combatant commanders must continue to ramp up their focus on the resilience of upstream assets and infrastructure, even if those assets are owned by others and lie outside their area of responsibility. Exercises can help support that transformation. Using severe but realistic scenarios to reflect the disruption of energy systems, transportation companies, and other infrastructure that near-peer adversaries can inflict, CCMDs and their partner components can assess potential effects on OPLAN execution. They can use these assessments to develop cost-effective options to address any MA shortfalls they identify.

Such reprioritization measures should be reflected in DOD budgeting systems. DOD leaders should examine a range of options to help build a culture of risk management that puts MA issues front and center in component and Department-wide investment and planning decisions, including:

- systematic efforts to remedy OPLAN-related MA shortfalls via the issue paper process
- use of the Joint Requirements Oversight Council system to strengthen MA
- modifications of the OPLAN development and review process to highlight (and develop options to mitigate) risks that adversaries will cripple OPLAN execution by striking essential installations and infrastructure.

In addition, DOD must develop MA strategies that better incorporate cross-cutting risks to MEFs, assets, and systems that span the domains of multiple Services and agencies. In the past, MA risk assessments too often focused on Service- or agency-specific concerns. Such narrow assessments cannot be simply aggregated to form a composite view of risks to OPLAN execution. A more joint (and more CCMD-led) approach will be crucial to counter asymmetric threats.

Finally, DOD must bring cybersecurity into the heart of mission assurance. The Department has made significant progress in moving beyond its traditional focus on "guns, guards, and gates" under DCIP and is accounting for a broader range of threats to mission assurance. DOD is also ramping up efforts to ensure that OPLANs can be executed even if cyber attacks disrupt the flow of grid-provided power to defense installations, ports, and the water systems and other infrastructure essential to their operations. DOD Instructions 8500.01, *Cybersecurity*, and 8510.01, *IT Risk Management Framework*, provide the policy foundations for these efforts. DOD Directive 3020.40 also emphasizes the need to integrate cyber issues into MA decisionmaking. However, the DOD catch-up process must accelerate to account for the growing severity and breadth of cyber challenges.

Expanding Partnerships with Critical Infrastructure Owners and Operators. Substantial policy support already exists for expanding P3s for both microgrids and accelerated power restoration for military bases. Both the 2012 MA strategy and DOD Directive 3020.40 emphasize the importance of partnering with the owners and operators of U.S. critical infrastructure, including the electric grid, to help ensure that the Department can perform its MEFs.

These policies have enabled the development of a growing number of P3s for installation microgrids as well as "outside the fence-line" initiatives to create redundant power feeds from the grid and other measures to strengthen the resilience of grid-provided power. DOD and its industry partners should continue to improve the ability of key defense installations to function as power islands segmented from the grid, with hardened on-site power generation, transmission, and distribution systems. DOD should also expand microgrid projects so that they can sustain service to water systems and other mission-critical loads in surrounding communities. Moreover, DOD and its industry partners should examine how these initiatives can be scaled up on a nationwide basis to help meet the intensifying cyber threat.

In addition to extending P3s for pre-event, steady-state collaboration and investments in grid resilience, DOD and industry need better plans and capabilities to coordinate operations in major events. A joint capacity for industry-government information-sharing will be a critical enabler. DOD should ensure that it has the appropriate mechanisms to receive data and malware threat signatures that these partners gather from operational technology logs (and vice versa), as well as assessments of potential risks to DOD-supporting infrastructure systems.

Industry and DOD have begun to consider enhancing such operational cooperation and coordination. During the GridEx IV exercise in November 2017, utility leaders expressed interest in exploring how the National Guard (operating in state Active-duty or full-time National Guard–duty [Title 32] status) might support state and local law enforcement and contractor security services to protect key substations and other grid assets from kinetic attack, including infrastructure that directly serves critical defense installations. Exercise participants and senior DOD leaders also discussed whether and how the National Guard might support utilities for post–cyber attack power restoration. DOD and its industry partners could further examine these cyber and physical security support options.

The private sector can also help DOD identify the specific critical assets and facilities that the Department depends on. The Federal Power Act provides the ideal point to move this effort forward. The act requires the Secretary of Energy, in consultation with other Federal agencies and grid owners and operators, to identify and designate "critical defense facilities" in the 48 contiguous states and the District of Columbia that are "(1) critical to the defense of the United States; and (2) vulnerable to a disruption of electric energy provided to such facility by an external provider."[28] Congress's definition of *defense critical electric infrastructure* also helps guide implementation of that requirement. Such assets include "any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]" as a critical defense facility, "but is not owned or operated by the owner or operator of such facility."[29]

DOD is already working with industry and DOE to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD also has

South Carolina Army National Guardsmen from 228th Signal Brigade out of Spartanburg, South Carolina, set up Joint Incident Site Command Center package to support Horry County Emergency Operations Center with back-up communications system, September 15, 2018 (U.S. Army National Guard/ Brian Calhoun)

a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.[30] However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure.

DOD will therefore need industry-government partnerships outside the electricity subsector. MA initiatives must account for cross-sector infrastructure interdependencies, as adversaries can also disrupt other infrastructure sectors that defense installations depend on. Specifically, DOD needs to make greater progress in addressing the risks of cascading failures across other civilian-owned infrastructure sectors, including water utilities, natural gas pipelines essential for power generation, and transportation systems that MEFs may depend on.

Many of these sectors are rapidly improving their cyber defenses and adopting industry standards to ensure sector-wide compliance. However, ports and other infrastructure critical to MA have traditionally focused on physical security rather than cyber resilience. DOD can partner with port owners and operators to help them meet their cyber challenges. In addition to sharing appropriate information on potential threats, the Department can help these owners develop and adopt standardized policies for assessing, containing, and mitigating cyber risks.[31]

DHS recently announced creation of its National Risk Management Center (NRMC), which can play a centralizing role for coordination between DOD and both industry and government partners in all sectors. The NRMC will be a locus for industry-government collaboration on sector-specific and multisector risk management efforts, including prioritization initiatives.[32] As noted by Tom Fanning, chief executive officer of gas and electric utility Southern Company, the center could also help enable DOD and the Federal Bureau of Investigation to play a uniquely critical role in protecting U.S. critical infrastructure: "hold[ing] the bad guys accountable."[33]

Supply Chains as a Special Area of Focus. Supply chain risks offer a particularly important opportunity for collaboration between DOD and industry. Adversaries could disrupt the grid by corrupting widely used infrastructure components then exploiting those common vulnerabilities to cause massive breakdowns.[34] This threat applies to all critical infrastructure sectors. Software, firmware, hardware, or network services are all vulnerable to supply chain compromise, potentially enabling adversaries to inject destructive malware and/or gain access to sensitive components and data in utility systems. Foreign ownership of technology companies poses an increasing threat due to potential ties to adversarial governments, especially for infrastructure in countries abroad that house U.S. bases.[35]

DOD is already working to combat this threat. Ellen Lord, Defense Under Secretary for Acquisition and Sustainment, recently noted that the Pentagon has compiled a "do not buy" list of software, in close collaboration with the Intelligence Community, to protect against Russian and Chinese supply chain threats.[36] Senior DOD officials have also noted that the Department will start red-teaming suppliers and contractors to ensure their cyber defenses are sufficiently robust.[37] While DOD is making important progress for securing its own infrastructure supply chains, it needs to work with industry to share threat information and develop shared approaches. Significant industry-government collaboration could yield a number of benefits, including a reduction in the duplication of costs and the ability to create the market incentives sufficient to ensure effective implementation.

DHS is currently leading industry-government collaboration efforts to address supply chain threats. Supply chain risk management will be a key focus of NRMC.[38] The House Homeland Security Committee also recently approved HR 6430, *Securing the Homeland Security Supply Chain Act*, which would authorize the Secretary of Homeland Security to enact a wide range of measures to curb supply chain risks, including the exclusion of specific vendors to support "urgent national security interest[s]."[39] Given the intensifying threat to cyber supply chains and the potential for widespread damage if an adversary successfully compromises critical and widely shared system components, DOD leaders should ensure that the Department is actively working with its industry and government partners on this issue moving forward.

Mission Assurance Abroad. DOD leadership should expand risk management for mission assurance on a global basis. Thus far, mission assurance has focused primarily on installations and supporting infrastructure in the United States. However, many OPLANs also depend on support from U.S. bases located in partner nations. China and other potential adversaries are rapidly expanding their ownership of (or provision of key operational control systems for) critical infrastructure worldwide, creating a growing threat vector to U.S. defense facilities and functions abroad. DOD's Operational Energy Strategy and Installation Energy Instruction provide valuable starting points to help address these issues and strengthen mission assurance.[40]

The Department of Defense is making rapid progress to strengthen mission assurance. However, adversary capabilities to disrupt the infrastructure that DOD depends on is growing at least as quickly. By focusing mission assurance on supporting combatant command operational plan execution, and expanding partnerships with critical infrastructure owners and operators, the Defense Department can stay ahead of the threat and continue to improve joint force lethality in the face of these asymmetric threats. JFQ

This article could not have been written without the research and editorial assistance of Rob Denaburg, Director of Security Research & Analysis, Sonecon LLC.

Notes

[1] The Department of Defense (DOD) defines *mission assurance* as a "process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the performance of DOD MEFs [mission essential functions] in any operating environment or condition." See *Mission Assurance Strategy* (Washington, DC: DOD, April 2012), available at <http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf>.

[2] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DOD, January 2018), 3, available at <www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[3] DOD defines *mission essential functions* as "Select functions directly related to accomplishing the Department's mission. Failure to perform or sustain these functions . . . would significantly affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control." See DOD Directive 3020.26, *DOD Continuity Policy* (Washington, DC: DOD, February 14, 2018), available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302026p.pdf>.

[4] *Mission Assurance Strategy.*

[5] DOD Directive 3020.40, *Mission Assurance* (Washington, DC: DOD, November 29, 2016), 3, available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf>.

[6] Julian Barnes, "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attack," *New York Times*, July 13, 2018, available at <www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html>.

[7] "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S. Computer Emergency Readiness Team (U.S.-CERT), March 15, 2018, available at <www.us-cert.gov/ncas/alerts/TA18-074A>; "Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S.-CERT, October 20, 2017, available at <www.us-cert.gov/ncas/alerts/TA17-293A>; Defense Science Board (DSB), *Task Force on Cyber Deterrence* (Washington, DC: DOD, February 2017), 4, available at <www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf>; ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats* (Fairfax, VA: ICF International, June 2016), 19.

[8] *Bricking* a piece of equipment means rendering it unusable, often due to firmware that is damaged beyond repair. See "Bricking," *Techopedia*, available at <www.techopedia.com/definition/24221/bricking>.

[9] SANS Industrial Control Systems and Electricity Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case* (Washington, DC: SANS Industrial Control Systems and Electricity Sharing and Analysis Center, March 18, 2016), 2, available at <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf>.

[10] "Alert (ICS-ALERT-17-206-01): CRASHOVERRIDE Malware," SANS Industrial Control Systems Cyber Emergency Response Team, July 25, 2017, available at <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01>; "Alert (TA17-163A): CrashOverride Malware," U.S.-CERT, June 12, 2017, available at <www.us-cert.gov/ncas/alerts/TA17-163A>; *CRASHOVERRIDE: Analysis of the Threat to Electric*

Grid Operations, Dragos, Inc., June 13, 2017, 8, available at <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>; and DSB, *Task Force on Cyber Deterrence*, 4.

[11] "Alert (TA17-163A)."

[12] *CRASHOVERRIDE*, 24.

[13] "Alert (TA18-074A)."

[14] Andy Greenberg, "Unprecedented Malware Targets Industrial Safety Systems in the Middle East," *Wired*, December 14, 2017, available at <www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/>; Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *New York Times*, March 15, 2018, available at <www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>.

[15] Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *Wall Street Journal*, July 23, 2018, available at <www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110>; "Alert (TA18-074A)."

[16] "Alert (TA18-074A)." Tim Conway, "Pictures and Theories May Help, but Data Will Set Us Free," SANS Industrial Control Systems, December 21, 2016, available at <https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free>; Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet," *WeLiveSecurity*, June 12, 2017, available at <www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.

[17] Chris Sistrunk, "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS Industrial Control Systems, January 8, 2016, available at <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>; Anton Cherepanov, "Win32/Industroyer: A New Threat for Industrial Control Systems," *WeLiveSecurity*, June 12, 2017, 15, available at <www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf>; "Alert (TA17-163A)"; *Quadrennial Energy Review—Transforming the Nation's Electricity System: Second Installment of the QER* (Washington, DC: Department of Energy, January 2017); "Destructive Malware," SANS Industrial Control Systems Cyber Emergency Response Team, March 2017, 1, available at <https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf>; "Alert (TA16-091A): Ransomware and Recent Variants," U.S.-CERT, September 29, 2016, available at <www.us-cert.gov/ncas/alerts/TA16-091A>.

[18] Greg Allen and Taniel Chan, *Artificial Intelligence and National Security* (Cambridge: Belfer Center for Science and International Studies, July 2017), 24, available at <www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>.

[19] "Aerial Drones Present Increasing Threat to Critical Infrastructure," The Foundation for Resilient Societies, April 16, 2015.

[20] *Grid Security Exercise: GridEx III Report* (Atlanta, GA: North American Electric Reliability Corporation, March 2016), available at <www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.

[21] Paul W. Parfomak, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, R43604 (Washington, DC: Congressional Research Service, June 17, 2014), 2, available at <www.hsdl.org/?abstract&did=755610>.

[22] *U.S. Department of Energy Electromagnetic Pulse Resilience Action Plan* (Washington, DC: Department of Energy, January 2017); Brandon Wales, *Oversight of Federal Efforts to Address Electromagnetic Risks*, Testimony Before the U.S. House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, May 17, 2016, 3–4, available at <http://docs.house.gov/meetings/HM/HM09/20160517/104869/HHRG-114-HM09-Wstate-WalesB-20160517.pdf>.

[23] *Guidance for DOD Utilization of Host Nation Power* (Lexington, MA: MIT Lincoln Laboratory, October 2015), 5, available at <www.dtic.mil/get-tr-doc/pdf?AD=AD1034495>.

[24] Jeffrey Marqusee, Craig Schultz, and Dorothy Robyn, *Power Begins at Home: Assured Energy for U.S. Military Bases* (Reston, VA: Noblis, January 2017), 5, available at <www.pewtrusts.org/~/media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf>.

[25] Tim Kelly, "U.S. to Bring Japan Under Its Cyber Defense Umbrella," Reuters, May 30, 2015, available at <www.reuters.com/article/us-japan-us-cybersecurity/u-s-to-bring-japan-under-its-cyber-defense-umbrella-idUSKBN0OF0EL20150530>.

[26] "U.S. Deeply Concerned Nord Stream Gas Link Is Security Threat," Reuters, May 6, 2016, available at <www.reuters.com/article/us-eu-gazprom-us/u-s-deeply-concerned-nord-stream-gas-link-is-security-threat-idUSKCN0XX1YG>.

[27] Kane Wu and Clara Denina, "UK Power Reserve Sale Attracts China's State-Owned Grids—Sources," Reuters, September 29, 2017, available at <www.reuters.com/article/uk-power-m-a/uk-power-reserve-sale-attracts-chinas-state-owned-grids-sources-idUKKCN1C4292>.

[28] See 16 U.S.C. § 824o-1, *Critical Electric Infrastructure Security*, § (c), available at <www.law.cornell.edu/uscode/text/16/824o-1>.

[29] See also 16 U.S.C. § 824o-1, § (a)(4).

[30] DOD Manual 3020.45, *Defense Critical Infrastructure Program* (Washington, DC: DOD, May 23, 2017), available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>; and DOD Directive 3020.40: *Mission Assurance* (Washington, DC: DOD, November 29, 2016).

[31] Daniel Trimble, Jonathon Monken, and Alexander F.L. Sand, "A Framework for Cybersecurity Assessments of Critical Port Infrastructure," in *2017 International Conference on Cyber Conflict* (Washington, DC, November 7–8, 2017), 1, available at <https://ieeexplore.ieee.org/document/8167506/>.

[32] "National Risk Management Center Fact Sheet," Department of Homeland Security, July 31, 2018, available at <www.dhs.gov/sites/default/files/publications/18_0731_cyber-summit-national-risk-management-fact-sheet.pdf>.

[33] Dustin Volz, "Pence Blames Russia for 2016 Election Interference, Vows to Tighten Cybersecurity," *Wall Street Journal*, July 31, 2018, available at <www.wsj.com/articles/dhs-forms-new-cyber-hub-to-protect-critical-u-s-infrastructure-1533029400>.

[34] *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, Mission Support Center Analysis Report (Idaho Falls: Idaho National Laboratory, August 2016), 20.

[35] *Foreign Economic Espionage in Cyberspace* (Washington, DC: National Counterintelligence and Security Center, July 2018), 12, available at <www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>.

[36] Roxana Tiron, "Pentagon's 'Do Not Buy' List Targets Russian, Chinese Software," *Bloomberg*, July 27, 2018, available at <www.bloomberg.com/news/articles/2018-07-27/pentagon-s-do-not-buy-list-targets-russian-chinese-software>.

[37] Marcus Weisgerber and Patrick Tucker, "Pentagon Creates 'Do Not Buy' List of Russian, Chinese Software," *Defense One*, July 27, 2018, available at <www.defenseone.com/threats/2018/07/pentagon-creates-do-not-buy-list-russian-chinese-software/150100/>.

[38] "National Risk Management Center Fact Sheet."

[39] "DHS Sets New ICT Supply Chain Task Force," *MeriTalk*, July 31, 2018, available at <www.meritalk.com/articles/dhs-sets-new-ict-supply-chain-task-force/>.

[40] *Department of Defense 2016 Operational Energy Strategy* (Washington, DC: DOD, May 2016, available at <www.acq.osd.mil/eie/Downloads/OE/2016%20DoD%20Operational%20Energy%20Strategy%20WEBc.pdf>; and DOD Instruction 4170.11, *Installation Energy Management* (Washington, DC: DOD, March 16, 2016), available at <www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/417011p.pdf>.

NDU Press Congratulates the Winners of the 2019 Essay Competitions

NDU Press hosted the final round of judging on May 16–17, 2019, during which 23 faculty judges from 13 participating professional military education (PME) institutions selected the best entries in each category. First Place winners in each of the three categories are published in the following pages.

Secretary of Defense National Security Essay Competition

The 13th annual competition was intended to stimulate new approaches to coordinated civilian and military action from a broad spectrum of civilian and military students. Essays address U.S. Government structure, policies, capabilities, resources, and/or practices and to provide creative, feasible ideas on how best to orchestrate the core competencies of our national security institution.

First Place
Mr. Daniel Hooey
Air Command and Staff College
"Pakistan's Low Yield in the Field: Diligent Deterrence or De-Escalation Debacle"

Second Place
Lieutenant Colonel Matt Gaetke, USAF
The Dwight D. Eisenhower School for National Security and Resource Strategy
"Mobilization in the 21st Century: Asking a Better Question

Third Place
Major Anthony Surman, USAF
Air Command and Staff College
"Eluding the Electromagnetic Chokepoint: 'For-Space' Intelligence to Enable Spectrum Maneuver"

Chairman of the Joint Chiefs of Staff Strategic Essay Competition

This annual competition, in its 38th year in 2019, challenges students at the Nation's joint PME institutions to write research papers or articles about significant aspects of national security strategy to stimulate strategic thinking, promote well-written research, and contribute to a broader security debate among professionals.

Strategic Research Paper

First Place
Mr. Andrew Rhodes
U.S. Naval War College
"The Second Island Cloud: A Deeper and Broader Concept for American Presence in the Pacific Islands"

Second Place
Commander Lloyd Edwards, USN
National War College
"Balancing Competition with Cooperation: A Strategy to Prepare for the Chinese Dream"

Third Place
Major Alvin Q. Chan, Singapore Army
Marine Command and Staff College
"China's 'Three Warfares': Insights into Cyberspace Competition and Potential U.S. Policy Options"

Strategy Article

First Place
Colonel James B. Cogbill, USA
U.S. Army War College
"America First ≠ America Alone: Morocco as Exemplar for U.S. Counterterrorism Strategy"

Second Place
Colonel Christopher A. Ingels, USA
U.S. Army War College
"Stabilizing Diplomacy in a Changing World Environment"

Third Place
Lieutenant Colonel Paul Golden, Jr., USA
U.S. Army War College
"Artificial Intelligence Revolution: Thoughts for Implementing an Effective Acquisition Strategy"

Joint Force Quarterly Maerz Awards

In its 4th year, the JFQ Maerz Awards, chosen by the staff of NDU Press, recognize the most influential articles from the previous year's four issues. Five outstanding articles were chosen for the Maerz Awards, named in honor of Mr. George C. Maerz, former writer-editor of NDU Press.

Forum
James Hasik
"Beyond the Third Offset: Matching Plans for Innovation to a Theory of Victory, "*JFQ* 91 (4th Quarter 2018)

JPME Today
Milan Vego
"The Bureaucratization of the U.S. Military Decisionmaking Process," *JFQ* 88 (1st Quarter 2018)

Commentary
Mike Jernigan and Jason Cooper
"Cooking Shows, Corollas, and Innovation on a Budget," *JFQ* 90 (3rd Quarter 2018)

Features
J. Patrick Work
"Fighting the Islamic State By, With, and Through: How Mattered as Much as What," *JFQ* 89 (2nd Quarter 2018)

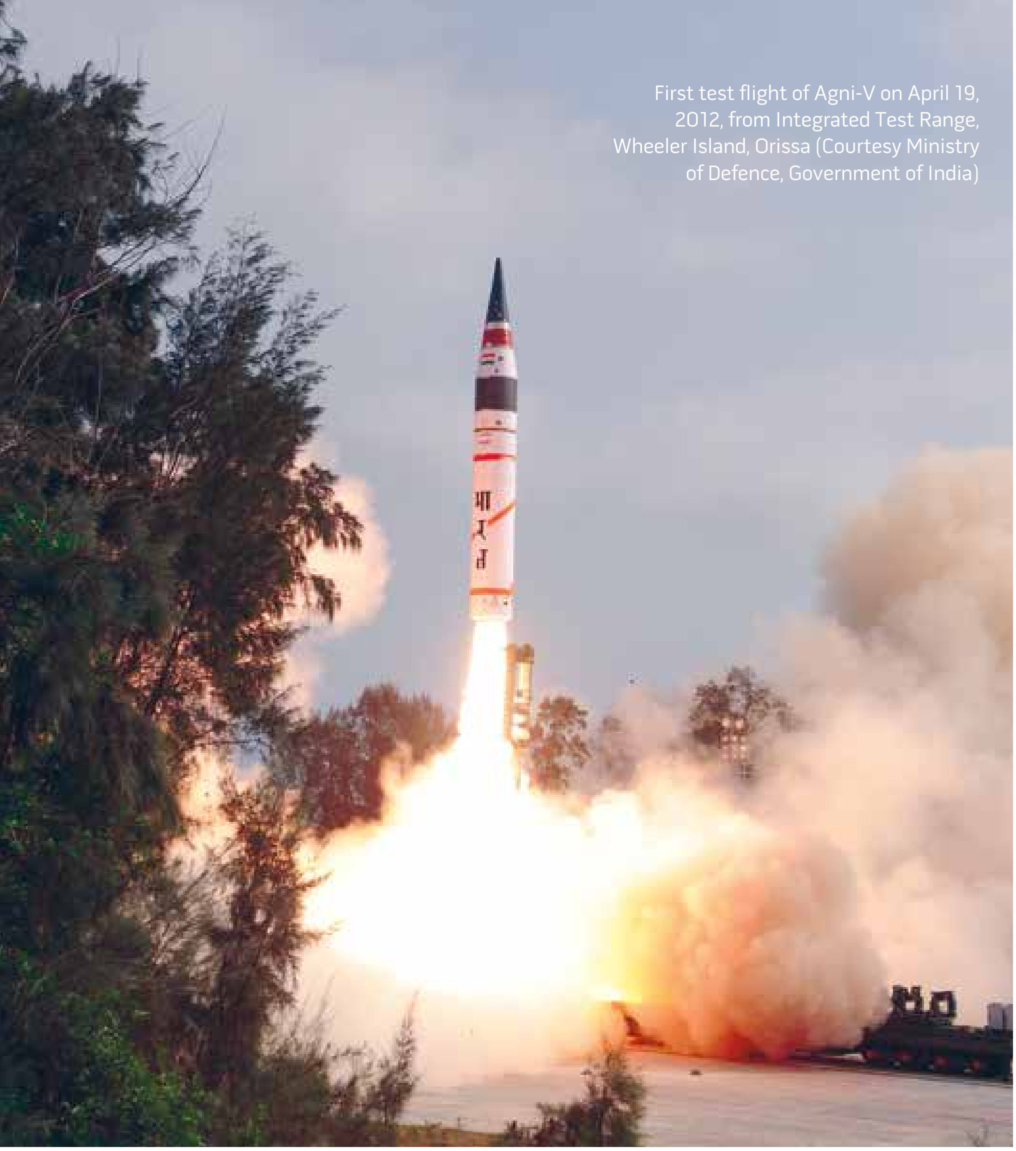
Recall
Kenneth T. "Max" Klima, Peter Mazzella, and Patrick B. McLaughlin
"Scipio Africanus and the Second Punic War: Joint Lessons for Center of Gravity Analysis," *JFQ* 88 (1st Quarter 2018)

Distinguished Judges

Twenty-three senior faculty members from the 13 participating PME institutions took time out of their busy schedules to serve as judges. Their personal dedication and professional excellence ensured a strong and credible competition.

Front row, left to right: Dr. Michelle Getchell, U.S. Naval War College; Colonel Donald Holloway, USAF, National War College; Dr. Amy Baxter, Air University eSchool; Dr. Donald W. Chisholm, U.S. Naval War College; Dr. Richard L. DiNardo, Marine Corps Staff College; General Joseph J. Dunford, Jr., Chairman of the Joint Chiefs of Staff; Dr. Charles Chadbourne, U.S. Naval War College; Dr. Elizabeth D. Woodward, Air War College; Dr. Benjamin "Frank" Cooling, Eisenhower School; Dr. C.J. Horn, College of Information and Cyberspace; Dr. Jeffrey D. Smotherman, NDU Press; Dr. Bonnie Calabria, College of International Security Affairs. Back row, left to right: Dr. John Terino, Air Command and Staff College; Dr. Paul Springer, Air Command and Staff College; Dr. Jeff Turner, Joint Forces Staff College, Dr. Naunihal Singh, U.S. Naval War College; Dr. James D. Kiras, School of Advanced Air and Space Studies; Dr. William T. Eliason, NDU Press; Dr. Peter Eltsov, College of International Security Affairs; Dr. Brian McNeil, Air War College; Dr. Ryan Wadle, Air University eSchool; Dr. James Chen, College of Information and Cyberspace; Dr. Jack Godwin, NDU Press; Dr. Jaimie Orr, National War College.

Not shown: Dr. Kristin Mulready-Stone, U.S. Naval War College; Dr. Larry D. Miller, U.S. Army War College; Dr. Daniel Marston, U.S. Marine Corps School for Advanced Warfighting. Photo by James Lewis, NDU.



First test flight of Agni-V on April 19, 2012, from Integrated Test Range, Wheeler Island, Orissa (Courtesy Ministry of Defence, Government of India)

Pakistan's Low Yield in the Field

Diligent Deterrence or De-escalation Debacle

By Daniel Hooey

Daniel Hooey wrote this essay while a student at the Air Command and Staff College. It won the 2019 Secretary of Defense National Security Essay Competition.

Having engaged in three wars and numerous border crises, Pakistan and India remain at a high state of potential conflict in the future; however, the prospects of escalation toward a nuclear exchange are a subject of rich debate among Western and South Asian scholars.[1] While the nuclear exploits of both countries trace back to the 1960s, this article focuses on developments observed since declared nuclearization in 1998—most notably Pakistan's ongoing pursuit of low-yield nuclear weapons (LYNWs).[2] The nuclear beginnings of both countries occurred clandestinely, outside the recognized "nuclear norms" of the five established nuclear-armed states.[3] These nuclear programs, born of failed nonproliferation efforts and viewed with ire by the international community, drew diplomatic pressure to sign nuclear treaties to conform with global efforts of inventory reductions, nuclear test bans, and disarmament. Having refused these overtures, both India and Pakistan continued to develop their nuclear programs, albeit toward seemingly different ends. India largely modeled its doctrine and behaviors after the established nuclear states, while Pakistan avoided the constraints of nuclear no first use and sought to proactively leverage the regional deterrence paradigm to its full advantage.

This article examines how Pakistan's pursuit of LYNWs has affected Indian and Pakistani conceptions of deterrence and escalation management and tests two independent hypotheses. The first hypothesis (H-1) asserts India will seek to maintain a credible second-strike nuclear posture and believes it can deter Pakistan's LYNWs with conventional forces and the threat of assured retaliation. The second hypothesis (H-2) asserts that Pakistan views LYNWs as a mechanism to lower the nuclear threshold as an instrument of brinkmanship.

This article employs a comprehensive approach to evaluate the two hypotheses using a body of Western and South Asian scholarly works that specifically pertain to the Indo-Pakistan nuclear paradigm. The article begins by outlining the respective nuclear doctrines and postures of both Pakistan and India and subsequently explores Pakistan's introduction of LYNWs and their impact on South Asian deterrence. Following this is an evaluation and testing of the two hypotheses, along with an assessment of the potential for a nuclear conflict in South Asia. The article culminates with sections exploring implications and opportunities for the United States and the international community.

Pakistan's Nuclear Doctrine and Posture

Pakistan's move toward LYNWs is believed to be predicated on observations of the U.S. employment of these systems in Europe during the Cold War.[4] The U.S. rationale for the employment of LYNWs was to deliberately lower the nuclear threshold to deter the possibility of Soviet aggression from adjacent Warsaw Pact nations.[5] Pakistan confronts similar challenges as it faces a conventionally superior Indian adversary. Conventional military asymmetry and an inability to compete with India economically render Pakistan incapable of addressing the widening military gap despite attempts to modernize and expand its military capabilities.[6] As such, it is unsurprising that Pakistan would turn to its nuclear arsenal, much like the United States did in Europe, for solutions to its lack of conventional parity.

Pakistan views its nuclear arsenal as the ultimate guarantor of its sovereignty and national survival against India, and its nuclear doctrine seeks to deter not only India's nuclear use but also the prospects of conventional aggression.[7] Though Pakistan has not officially declared a nuclear doctrine, instead invoking principles of selective ambiguity, Islamabad's policies and actions since 1998 have revealed its core tenets.[8] South Asian scholars such as Gurmeet Kanwal posit that "ambiguity has been used as an offset for conventional inferiority with the belief that control over escalation is possible."[9] Pakistan's nuclear doctrine encompasses four primary principles: Indo-centric minimum nuclear deterrence, massive retaliation (although its limited arsenal may not lend itself to such), nuclear first use, and strategies that emphasize countervalue nuclear targeting.[10] While Pakistan's nuclear posture has shifted in response to regional threat perceptions, there has been little observable change to its salient doctrinal features.

Pakistan operates under a true nuclear dyad with India, which allows Islamabad to focus its entire nuclear contingent against a single adversary. The associated regional dynamics pose unique challenges given the geographical contiguity of the two countries. The associated lack of geographic depth inherently alters the nuclear dynamics between these states and complicates nuclear employment and doctrinal considerations.[11] While Pakistan claims a policy of minimum deterrence, this is more likely out of necessity than choice. As opposed to India, which deliberately chooses to limit the size of its nuclear arsenal, Pakistan is forced to do so given the budgetary and fissile material production constraints that have limited its nuclear ambitions.[12]

Massive retaliation is a key facet of Pakistan's nuclear doctrine, although its limited arsenal probably lends itself more toward assured retaliation by Western standards. South Asian scholars believe this is driven by two factors: the need to deter a potential Indian preemptive strike against its nuclear arsenal, and to offset its conventional inferiority.[13] Pakistan's progression toward a nuclear triad and concerns over India's burgeoning ballistic missile defenses are testaments to Islamabad's doubts in the credibility of its second-strike capabilities and will serve as a justification for a larger and more diverse arsenal.[14] Experts believe Pakistan is rapidly expanding its arsenal, which could eventually put it on pace to surpass the United Kingdom and France in terms of its inventory; however, Pakistan may exhaust its sources of uranium ore by 2020, putting it at an upper limit of around 250 strategic weapons.[15]

Pakistan's selection of nuclear first use was an obvious choice given its lack of conventional parity with India, which has required Islamabad to threaten the use of its full nuclear complement to buttress its nuclear credibility. It is important to note that this inherently makes Pakistan more prone to consider the use of nuclear weapons as a warfighting capability, which in part explains Islamabad's pursuit of LYNWs. The fact that many of Pakistan's key cities are within striking distance of the border also heightens Pakistani perceptions of strategic vulnerability, making the prospects of first use more appealing as it offers more flexibility. Enduring concerns over the survivability of its second-strike capabilities and, more recently, India's advancements in missile technology to include hypersonic variations of its Brahmos II continue to make nuclear first use the most viable option.[16] The "use it or lose it" dilemma faced by countries that typically adopt first-use postures will similarly challenge Pakistan as LYNWs will be subject to these issues.[17]

There are several factors that shape Pakistan's doctrine regarding countervalue targeting. The relatively small size of Pakistan's nuclear arsenal makes it important to maximize punishment on New Delhi, which is likely why Islamabad (perhaps mistakenly) terms it a policy of maximum retaliation. Neither India nor Pakistan possess a sufficient arsenal to achieve the Cold War measure of mutually assured destruction, but both possess the ability to destroy large swathes of each other's territory. However, India's strategic depth, combined with the lack of reach of Pakistan's weapons (although this is improving), would render efforts to preemptively attack Indian strategic assets ineffective, thus giving Pakistan little hope of achieving a successful decapitation while simultaneously subjecting it to assured retaliation from India. Indian population and industrial centers are within striking distance of Pakistani nuclear weapons, making them lucrative targets that are easy to engage.[18]

The most substantive examination of South Asian nuclear postures is derived from the analysis of U.S. scholar Vipin Narang. He asserts that Pakistan started with a more stable catalytic posture that relied on the intervention of a third-party patron (initially the United States).[19] However, the rather tumultuous nature of the U.S.-Pakistan relationship over the years—one that has been fraught with mutual distrust and perceptions of U.S. strategic abandonment—led to an eventual shift toward a more dangerous and unstable asymmetric escalation posture.[20] The exact state of Pakistan's nuclear readiness is unknown, but Islamabad claims it maintains a low state of readiness with its warheads stored at dispersed locations in a disassembled state.[21] While Pakistan's strategic systems are not believed to be stored in a ready state, this may not apply to its developing LYNWs. The air-, sea-, and ground-launched cruise missile variations of Pakistan's low-yield systems are believed to be produced and stored in a fully assembled state.[22] Pakistan claims it has no plans to proactively disperse its low-yield systems, which is unsurprising as doing so would invite preemptive or preventative strikes by India. However, it does make it clear that these systems are stored in a manner that allows them to be deployed quickly during a crisis, alluding to a period of hours, not days.[23]

India's Nuclear Doctrine and Posture

U.S. scholar and recognized authority on Indian nuclear doctrine Ashley Tellis posits that "any discussion of India's nuclear doctrine and force posture is by definition fraught with uncertainty" and something that could take decades to sort out.[24] Tellis notes that doctrine progresses at the unpredictable pace of technological advancement, and this, along with other conditions that prompt rapid change, may be the case with Pakistan's introduction of LYNWs.[25] India released its *Draft Report of the National Security Advisory Board on Indian Nuclear Doctrine* on August 17, 1999, which represented the most comprehensive document on Indian nuclear doctrine that New Delhi has ever produced.[26] Many experts claim there has been little change to the core tenets of the doctrine since the draft was released, but Tellis cautions the draft was written to serve as recommendations that do not necessarily reflect established policy.[27] From its inception, the policy was not only provocative for Pakistan and China but also highly contested internally.[28]

A largely unchanged version of the doctrine released in 2003 included key concepts of no first use, minimum credible deterrence, and assured retaliation. According to Vipin Narang, the overriding intent of India's doctrine is to "deter the use and threat of use of nuclear weapons by maintaining an adequate retaliatory capability should deterrence fail."[29] Many scholars believe this posture implies that India will absorb the first nuclear blow and will invoke its doctrine of assured retaliation to authorize a strategic nuclear response.[30] It is this point that draws contention among contemporary critics of no first use, who assert this weakens India's deterrence credibility. However, Tellis notes that this concept is "remarkably pervasive in Indian strategic thought," which may explain why this policy has endured despite prolonged disputation.[31] India's doctrine also calls for minimum credible deterrence seeking to achieve deterrent effects with a limited arsenal.[32] There are indications, though, that India, like Pakistan, considers the size of the arsenal to be a fluid concept that must be responsive to the actions of its adversaries.[33] As Pakistan and China expand and diversify their arsenals, it is reasonable to assume India will also do so in kind to maintain its deterrence credibility.

Assured retaliation is a significant, although also highly contested, aspect of India's nuclear doctrine. India does not consider nuclear weapons as warfighting options, but as instruments of punishment to inflict maximum damage against an adversary should deterrence fail.[34] Tellis further qualifies this concept as "delayed, but assured, retaliation." Since India is postured for punitive operations, it must therefore consider that the ability to retaliate is more important than the timing of the response.[35] While there is no specified timeline for a nuclear response, it must be assumed that India will be required to calculate its reaction, ready the required delivery vehicles and warheads, and execute the nuclear command, control, and communication (NC3) authorization process. While there are indications that India has enacted measures to reduce nuclear response times, there is a reasonable expectation for delay due to New Delhi's highly centralized NC3 structure. Given that India's doctrine restricts nuclear use to punishment, Tellis and others assess that nuclear weapons will be directed against primarily countervalue (civilian) targets.[36] This is further evidenced by India's proclivity to use these weapons toward achieving political ends rather than military objectives on the battlefield.[37] As such, Tellis concludes, "India is almost certain to settle for countervalue targeting and, by implication, seek to service a nuclear strategy centered on some kind of mutual assured vulnerability."[38]

Narang offers useful insights into India's nuclear posture noting three specific pillars of its nuclear policy: no first use, assured massive retaliation, and under "no condition will the weapons be conventionalized."[39] Under these pretenses, Narang's model categorizes New Delhi's nuclear posture as one of assured retaliation. While India lacks the strategic reach to target the entirety of Chinese or Pakistani territory, it retains the ability to inflict substantial damage against either state, which substantiates its deterrence credibility, and its technological advancements are quickly narrowing this gap.[40] Despite some indications of internal debate, there are no signs that India has officially altered any facets of its existing nuclear posture or doctrine in response to Pakistan's threats of LYNWs.

Low-Yield Nuclear Weapons Deterrence

LYNWs, in nearly every facet of employment, tend to complicate traditional concepts of deterrence and necessitate considerations of limited nuclear war. U.S. nuclear scholars such as Jeffrey Larsen and Kerry Kartchner have assessed and evaluated the many challenges associated with the possibility of limited nuclear war—a prospect so dangerous that the United States and the former Soviet Union bilaterally agreed to abandon these practices in Europe.[41] As Lawrence Freedman famously wrote, "It takes two to keep a war limited," a lesson that no doubt applies to the South Asian dynamic, perhaps in more striking ways. At face value, the animosity between the two countries is not so different from other adversarial relationships in the international system, but what makes this rela-

Military truck carrying intermediate-range ballistic missile of Pakistani army, November 27, 2008 (Courtesy SyedNaqvi90)

tionship different is that all major crises since nuclearization have required a degree of international mediation assistance.[42] The fact that these countries do not effectively engage on a state-to-state level—even during periods of enormous bilateral tension—creates an obvious deterrence issue, decreasing the probability of effective communication of nuclear signaling or de-escalation measures during the progression of a crisis.[43] These challenges are exacerbated by a heightened potential for confirmation bias during a crisis given the inability of both sides to objectively detect, process, and validate the intentions of the other. A lowered nuclear threshold and the decentralized nuclear authority structure inherent to LYNWs will inevitably reduce decision space for senior leaders on both sides, which could make this a recipe for disaster.

Driven by its development and ongoing integration of LYNWs, Pakistan has adopted its doctrine of full-spectrum deterrence, which seeks to lower the nuclear threshold to provide Islamabad the flexibility to contend with even conventional threats from India.[44] Indian scholar Inderjit Panjrath notes four central themes that are apparent in official Pakistani statements regarding full-spectrum deterrence. First, LYNWs were a response to India's Cold Start doctrine that seeks to rapidly conduct numerous limited military penetrations to secure Pakistani territory while remaining under the nuclear threshold. Second, Pakistan acknowledges that any battlefield use would have strategic consequences. Third, full-spectrum deterrence is not a warfighting strategy, but rather a strategy to deter limited conventional war below Pakistan's existing threshold for nuclear use. Fourth, Pakistan will maintain centralized command and control of LYNWs in the same manner as its strategic arsenal.[45] While superficially reassuring, these endeavors tend to alter the deterrence paradigm between the affected states as observed during the similar introduction of LYNWs in Europe during the Cold War. As Dave Smith surmised, "Pakistan's decision to embrace tactical nuclear weaponry will ultimately require it to deal with the doctrinal implications, increased security and command and control requirements, and the potentially destabilizing implications of deploying such weapons."[46]

Pakistan's development of a low-yield triad to increase the credibility of its second-strike capability will further disrupt the deterrence paradigm and could hasten reciprocal Indian efforts to acquire comparable capabilities to defeat Pakistan's systems. These developments were probably a component of India's ongoing pursuit of a viable ballistic missile defense system, which threatens the credibility of Pakistan's strategic delivery vehicles. Such developments will inevitably invoke further South Asian arms races; however, India's economic and already significant qualitative and quantitative military advantages will increasingly widen the gap and stimulate further Pakistani strategic paranoia. This dichotomy is unsustainable for Islamabad, whose failing economy will continue to stunt its military development and nuclear ambitions. Unlike India, whose conditional Nuclear Suppliers Group status grants New Delhi the ability to purchase nuclear materials, Pakistan's inability to secure additional fissile material from external sources will significantly hamper its future efforts.

Another change to the deterrence paradigm stems from the potential for dispersal and the NC3 structure for LYNWs. There are indications that Pakistan actively employs denial and deception measures and routinely shuffles its strategic nuclear assets among a dozen or more secret bunkers in addition to several other phony locations.[47] There are also suspicions of various decoy sites in an elaborate tunnel network to optimize the prospects of survivability.[48] An intermingling of conventional and nuclear-tipped delivery systems, coupled with elaborate denial and deception mechanisms, could inadvertently provoke an Indian preventative strike if these systems were dispersed during a crisis regardless of the type of munition used.[49] The other issue concerns the NC3 of LYNWs, as Inderjit Panjrath observed that "pre-delegation to field commanders was an integral part of credible deterrence through TNWs [tactical nuclear weapons]."[50] U.S. scholars echo these concerns as they identify Pakistan as one of the few nuclear states that has adopted such a structure.[51] Delegative NC3 postures provide advantages as they diversify launch authority, which negates the prospects of a decapitation strike and allows for rapid assembly, deployment, and delivery of nuclear weapons during crisis situations while providing few physical barriers to their release.[52] However, these postures also tend to introduce increased potential for miscalculation, nuclear accidents, or inadvertent and/or unauthorized use.

India's Reaction to Full-Spectrum Deterrence

The various works of South Asian and Western scholars suggest India may be struggling to cope with the prospects of full-spectrum deterrence. Indian discord over full-spectrum deterrence is confined to two primary spheres of thought: nuclear pessimists who advocate for an alteration of India's current doctrine to address the prospects of full-spectrum deterrence, and nuclear optimists who believe full-spectrum deterrence can be mitigated through existing means without the need to alter or adapt existing doctrine. Each side presents a relatively strong case to substantiate its respective claims, but there are also areas of convergence between the two camps.

Nuclear pessimists contest that India's doctrinal concepts of no first use and assured retaliation make New Delhi vulnerable to acts of Pakistani provocation, essentially rendering India strategically paralyzed.[53] While India's current doctrine of assured retaliation reserves the right to use nuclear weapons if any weapons of mass destruction are used on any Indian forces anywhere, pessimists believe this may be insufficient to deal with full-spectrum deterrence.[54] Pessimists have also called for the Indian military to develop a reciprocal low-yield capability to allow for a proportional response should Pakistan detonate LYNWs during a future crisis or conflict.[55] There has also been significant emphasis on developing a robust ballistic missile defense capability that is seemingly based on Israel's Iron Dome model. New Delhi has acquired several of the components of the system, such as the Green Pine radar and associated interceptor missile systems, from Tel Aviv.[56] While the broader Indian political community considers its nuclear arsenal purely strategic, there are indications that New Delhi may be trending toward a higher state of readiness. Vipin Narang notes India may be pursuing avenues such as "canisterization," which is a method of hermetically sealing and storing a fully mated warhead to reduce preparation timelines during future crises.[57]

Nuclear optimists tend to downplay the threat of full-spectrum deterrence, instead highlighting the benefits of adhering to India's existing doctrine. They argue that India capitalizes on the benefits of its recognition as a responsible actor within the international community by ignoring Pakistan's provocative actions. These efforts, in no small part, helped secure India's conditional entry into the Nuclear Suppliers Group and may outweigh the risks of electing not to respond.[58] Extensive studies have also revealed the ineffectiveness of LYNWs against advancing armor columns, which is what many Indian military experts assess to be the primary target of Pakistan's LYNWs.[59] It would take hundreds of these systems to destroy a single armored division, which would quickly exhaust Pakistan's LYNW inventory and inevitably incite an Indian reprisal in the form of a full-scale nuclear retaliation with its strategic assets.[60]

In addition, LYNWs would place high demands on Pakistan's existing plutonium stocks, as these systems require a significant amount of fissile material to produce and would be capable of achieving only marginal effects on the battlefield.[61] These are considerations that prompt some optimists to label these systems "showcase weapons" rather than viable warfighting systems.[62] Optimists also posit that, regardless of the promises of full-spectrum deterrence, there is still room under the nuclear umbrella for conventional military action. The "surgical strikes" conducted by Indian special forces in September 2016 in response to the Uri terrorist attacks are cited as evidence, as full-spectrum deterrence had been implemented by this time.[63]

Both sides agree on several core issues, including actively exploring ways to mitigate Pakistan's ability to export terrorism under the umbrella of nuclear blackmail.[64] Both camps also seem to agree that the political space for Indian restraint in the face of continued terrorist attacks emanating from Pakistani soil is rapidly diminishing—a point that Western scholars are also concerned about.[65] Hardliners within India's current Narendra Modi government have

Admiral Phil Davidson, commander of U.S. Indo-Pacific Command, hosts India's Minister of Defense, Nirmala Sitharaman, on barge tour of historic Pearl Harbor, Hawaii, December 6, 2018 (U.S. Navy/Robin W. Peak)

popularized the prospects of assuming a firmer stance regarding Pakistan that may progressively drive the political establishment toward more provocative responses to preserve political capital in the future.[66] Another area of convergence involves addressing issues with Pakistan in a manner that preserves India's positive image in the international community.[67]

Low-Yield Rationale: Pakistan Coping with Asymmetry or Strategic Brinkmanship?

This section evaluates the two hypotheses pertaining to the insertion of LYNWs into the South Asian nuclear context. The first hypothesis asserts that India will seek to maintain a credible second-strike nuclear posture and believes it can deter LYNWs with conventional forces and threat of assured retaliation. The second hypothesis asserts that Pakistan views LYNWs under its policy of full-spectrum deterrence as a mechanism to lower the nuclear threshold as an instrument of brinkmanship.

H-1 attempts to explain how India would cope with the introduction of LYNWs as New Delhi must contend with two nuclear-armed adversaries in both Pakistan and China. Despite recent debate over some facets of India's doctrine, no significant changes have been made to its core tenets since its drafting in 1999 regardless of Pakistan's intent to field LYNWs. Most experts seem satisfied with the guarantees of India's existing doctrine of assured retaliation, which calls for a strategic response to the use of weapons of mass destruction against Indian forces operating anywhere. While there are scholars who advocate for India to develop a reciprocal low-yield capability, there is no evidence that India has developed a low-yield equivalent or even intends to do so. The preponderance of Western and South Asian scholars agree that LYNWs do not pose a significant threat to advancing armor forces and do not significantly improve deterrence credibility based on empirical evidence from the U.S. experience in Europe and assessed conditions in South Asia.[68] Indian and Western scholars surmise that, like the U.S. employment of LYNWs in Europe, these systems are not meant for battlefield use and are more of a "showcase weapon" with limited range and yield.[69] Indian and Western scholars also agree that the tremendous fissile material commitments for these weapons make them unlikely to be widely fielded and, if proactively dispersed, would be easy targets of Indian preemptive strikes.[70] Indian scholars such as Inderjit Panjrath also believe there is still room for conventional actions under the nuclear umbrella, citing the surgical strikes conducted after Uri.[71]

In addition, there is evidence that India is continuing to improve its second-strike credibility through the acquisition of nuclear submarines and development of advanced delivery vehicles.[72]

While a large body of evidence supports H-1, there is also contradictory evidence that counters this claim. Both Western and South Asian scholars assess that Indian tolerance for continued attacks by Pakistani terrorists is diminishing and, with it, prospects of strategic restraint. While India has elected to curb its present response to LYNWs, this sentiment may not prevail in the long term, particularly given growing concerns of nuclear blackmail. Hardliners in the existing Modi government have popularized a hard stance, a trend that is expected to continue as future politicians campaign for office, which may lead to gradual changes to India's nuclear posture. There is a body of nuclear pessimists that is calling for changes to the existing nuclear doctrine, most notably its policies of no first use and assured retaliation; however, these calls do not appear to reflect the sentiments of civilian government personnel who would be the only officials empowered to alter the doctrine.[73] While this has not yet prompted any observable doctrinal changes, additional crises or provocative actions by Pakistan could give these arguments more traction to incite future modifications.

H-2 seeks to explain Pakistan's rationale and endstate for the development of nuclear weapons. There is strong evidence to support the first portion of H-2, which asserts full-spectrum deterrence seeks to lower the nuclear threshold, as Pakistani officials claimed this was exactly what these systems were intended to do. Western and South Asian scholars largely agree that Pakistan is following the model set forth by the U.S. employment of LYNWs during the Cold War as a means of deliberately lowering the nuclear threshold. There is also evidence that indicates these weapons may be intended not for battlefield use, but rather as standoff weapons like those deployed by the United States in Europe. There is no evidence that refutes the use of LYNWs to lower the nuclear threshold. There are, however, significant challenges associated with H-2.

The difficulty with proving or disproving H-2 relates to the second portion of the hypothesis, which deals with nuclear brinkmanship. While the introduction of LYNWs carries numerous inherent risks and the potential for brinkmanship, there is no evidence to suggest that Pakistan has leveraged them, or even intends to leverage them, for deliberate escalatory actions. Pakistan certainly realizes that provoking an Indian strategic nuclear response would invoke destruction of the Pakistani state, but this realization may not stop Islamabad from manipulating the conditions during an escalation in hopes of obtaining concessions from India. While LYNWs may not be deliberately intended to create the conditions for brinkmanship, there may be opportunities for such exploitation to occur as a crisis evolves. Indian scholars openly accuse Pakistan of shielding terrorism with nuclear blackmail, and, while perhaps not entirely untrue, there is little more than Indian accusations to substantiate this claim. The preponderance of evidence suggests that Pakistan, concerned over the reduced credibility of its deterrence against a conventionally superior adversary, has simply leveraged its most powerful instrument of war to address perceived conventional gaps. While it does so in a conceivably dangerous manner, this is not evidence of brinkmanship.

In sum, research validates H-1, as the bulk of the evidence suggests that India has not deviated from its existing strategies in response to LYNWs. There could be a variety of drivers for this, but there seems to be a prevailing sentiment that India has much more to lose with regard to international credibility by responding in a manner that would be perceived as irrational. There are no indications that deterrence considerations concerning China have substantively affected India's calculus regarding LYNWs, and New Delhi seems comfortable with its existing deterrence posture, aided by natural defensive terrain advantages along its northern border.[74] Per the available evidence, the results of H-2 are inconclusive. While the aspects of lowering the nuclear threshold are not in question, the subsequent prospects of nuclear brinkmanship have not been definitively proved. There is little evidence to suggest Pakistan is deliberately engaging in nuclear brinkmanship; however, there is nothing saying that it has not or will not do so in the future.

Assessing the Potential for the Great Nuclear Misadventure

While it is easy to dismiss the enduring problems between India and Pakistan as merely a regional issue that can be worked out bilaterally, the effects of even a limited nuclear conflict carry grave consequences that extend far beyond the region. U.S. scholars offer a grim and sobering view of what LYNWs could mean in the South Asian context. The United States previously reached similar conclusions about LYNWs in Europe as initial wargames and exercises in the 1950s revealed that "in only 9 days of simulated nuclear combat, West Germany was judged to have suffered three times the civilian casualties of [World War II]."[75] Historic assessments have shown the consequences of even the most limited nuclear exchange are far reaching and produce a strategic effect regardless of yield. LYNWs introduce additional factors that must be carefully considered, such as increased potential for miscalculation, nuclear accidents, unauthorized use, and impacts to the intervention calculus, which will be explored further below.

One of the more difficult challenges of LYNWs is their inherently destabilizing nature, exacerbated by Pakistan's propensity toward nuclear ambiguity that in turn creates an environment rife with miscalculation potential. While Pakistan and India have successfully maneuvered their way through various crises and international incidents over the years using a bilaterally understood framework of escalation management, the introduction of LYNWs may have a significant impact on the calculations of both countries. Given that Pakistan's ground-based LYNWs are considered dual-use systems with conventional and nuclear-tipped munitions, even a benign deployment of high-explosive–equipped systems could cause a significant overreaction by India, which may misperceive such systems as an escalation to a nuclear level.[76] Pakistan could also elect to intentionally deploy conventional low-yield systems (real or decoy) to attempt to coerce India to stand down during a period of heightened tensions, leveraging these systems as a dangerous instrument of battlefield signaling.

Another key facet of miscalculation involves target selection. As mentioned, Indian scholars have wrestled internally with the doctrinal prospects of assured retaliation, which do not adequately address the threat of LYNWs.[77] As such, questions arise as to what response options India would contemplate in the event Pakistan actually employed such systems during a crisis.[78] Will it matter if Pakistan uses LYNWs against advancing Indian forces on its own soil? Does countervalue (civilian) versus counterforce (military) targeting make a difference in the Indian calculus? Given that India does not possess an LYNW equivalent, does proportionality matter enough to prevent them from using a strategic weapon in response? The fact that New Delhi itself does not have clear answers to these difficult questions should theoretically give Pakistan pause to carefully evaluate how it employs such assets; however, this does not appear to be the case.[79]

The second factor involves the potential for accidental or unauthorized use. U.S. scholars like Eric Schlosser conclude that sustaining a high level of nuclear alert creates the conditions for an "always/never" dilemma.[80] Under these conditions, nuclear weapons are expected to always work when called upon and never fail. Western scholars have expressed serious doubt regarding the safety measures of low-yield delivery vehicles as such systems are expected to be made field-expedient for rapid use on order—these circumstances favor the "always" to the detriment of the "never."[81] There is also a question as to whether Pakistan's LYNWs have been subjected to the same level of safety scrutiny as its strategic systems, namely weapons that are one-point safe.[82] The absence of strong safety controls and centralized authorization mechanisms during crises makes the weapons not only less safe (accidental use) but also vulnerable to unauthorized use.[83] Pakistan has a demonstrated vulnerability to insider attacks as evidenced by the assassination of the Punjab governor by members of his own security detail, various unsuccessful assassination attempts against President Pervez Musharraf, and numerous attacks against Pakistani military installations.[84] While there are stringent personnel evaluation controls in place to actively monitor members of Pakistan's nuclear community, it is unknown to what degree these measures are applied to crews operating the various components of Pakistan's LYNW arsenal. The delegative nature of the NC3 authority for LYNWs places high decision capital on relatively junior military officers in the field, which could create the conditions for a "rogue major" to take actions into his own hands without authorization.[85] Even under prudent operational control, a junior officer may quickly face a "use it or lose it" scenario during an Indian counteroffensive as the limited range of these systems requires them to be positioned close to the border, outside the hardened defenses of the rear garrisons.[86]

The final factor is the potential effects of LYNWs on the international intervention calculus. Both countries have adopted conventional military strategies that attempt to inflict (in India's case) or deflect (in Pakistan's case) as much conventional punishment as possible prior to international intervention.[87] India's Cold Start doctrine, more recently labeled Proactive Strategy, seeks to rapidly conduct numerous limited military penetrations to secure Pakistani territory while remaining under the nuclear threshold.[88] Many South Asian scholars assert this strategy was a major driver of Islamabad's push toward LYNWs, even though the strategy was never officially adopted by India.[89] In response, Pakistan has since developed a strategy called New Concepts of Warfighting, which seeks to "modernize, restructure and re-position its armed forces" to blunt Indian advances in conjunction with its LYNWs.[90] Former Pakistani strategic plans division commander Lieutenant General (Ret.) Kahlid Kidwai claimed LYNWs were intended to "pour cold water on Cold Start."[91] What is most striking about the Indian and Pakistani war plans is the strong emphasis on speed of execution. While on the surface this represents prudent military planning by both militaries to optimize force agility, these endeavors also critically limit decision space and de-escalation potential. The tempo of conflict that these strategies hope to achieve increases the potential for a rapid escalation sequence, while decreasing space for bilateral de-escalation measures to occur. Timely international intervention becomes more complicated under these expedited escalation timelines. There is also the potential that a military crisis under these conditions could unravel so quickly that an international intervention may not occur in time to prevent a nuclear first-use scenario.[92] Should this scenario play out, the prospects of convincing India to exercise restraint and withhold a strategic nuclear response against Pakistan become exceedingly slim. These issues, if left unchecked, may spell out the very nuclear disaster that many Western scholars adamantly fear, and with it a host of implications that will be explored further in the next section.

Implications for International Intervention

The complex nature of the dynamics between India and Pakistan as nuclear-armed opponents poses unique risks on the world stage and foments distinctive challenges for the international community. International intervention is a calculated component by both India and Pakistan during these crises as a mechanism to draw in patron support.[93] This is exemplified by U.S. scholar Mooed Yusuf's observation that "the predictability of U.S. crisis interventions also created a moral hazard problem and an incentive for Pakistan and India to manipulate the risk of war to attract Washington's attention and support."[94] These conditions demand a more multilateral approach with an emphasis on mediation to manage tensions and control incidents of potential escalation. Yusuf offers an insightful approach to this problem, which involves the use of third-party brokering techniques. All three military crises between India and Pakistan since declared nuclearization were dependent on some form of third-party intervention to facilitate de-escalation.[95] The paragraphs that follow evaluate Yusuf's model, explore the individual roles of the United States and China, and examine the prospects of a quadrilateral approach to future crises.

Yusuf relates brokered bargaining to a three-actor model that explains state behaviors during various crises.[96] The model is comprised of two parallel and intertwined interactions. The first involves the antagonists aiming actions and signals at one another in hopes of deterring an outcome or compelling them to respond in line with crisis objectives. The second involves luring the third party to act in certain ways while the intermediary attempts to find space to mediate to defuse the crisis.[97] These interactions ultimately lead to "an interplay of the perceptions, expectations, incentives, and strategies among the three parties that affects the overall behavior and stability, and in turn, the outcome of a crisis."[98] This results in a competition of sorts between the antagonists to obtain third-party support rather than a fear of a rebuke or third-party action against them.[99]

Yusuf's model did not specifically address Pakistan's pursuit of LYNWs and instead focused on de-escalation short of a descent into nuclear war. While this will certainly be the most prudent approach to prevent the use of such weapons short of all-out mobilization, care must also be given to quick de-escalation. Pakistan's development of a low-yield triad, and its intent to leverage LYNWs as a means to lower the nuclear threshold, also raise the potential for escalation to occur sooner in the conflict.[100] Traditional second-strike options require proactive deployment early in a crisis for survivability, and Pakistan's development of nuclear-capable subsurface LYNWs for its fleet of *Agosta*-class submarines could stimulate the conditions for an early nuclear exchange.[101] Observed deployment preparations of conventional variants of these low-yield systems alone could prompt India to escalate during a crisis. The public fear that such a scenario would invoke may also severely limit New Delhi's decision space and timing. The lack of an obvious solution to such problems increases the need for proactive intervention from the international community, most notably from the United States and China.

The United States has played a predominant role in the de-escalation process during previous crises in South Asia. It has been able to accomplish this through a careful process of leveraging existing transactional partnerships with Pakistan while simultaneously appealing to India's desire to be perceived as a growing international power by urging New Delhi to exercise restraint.[102] While this approach has worked well in the past, Washington's growing discord with Islamabad, namely over its alleged support to terrorism in Afghanistan, coupled with dwindling international aid may reduce U.S. clout during future intervention efforts.[103]

Growing U.S. ties with India since 2005 and Pakistan's fears of strategic encirclement via perceptions of U.S. encouragement of an India-friendly Afghan government in Kabul have only further diminished the U.S. ability to influence Islamabad.[104] Inderjit Panjrath also alludes to the possibility that the bilateral relationship could turn adversarial when he posits that "Pakistan's attitude toward the U.S. and its allies in Afghanistan may turn hostile, further exacerbating the already fragile situation and adding yet another dimension to the ongoing conflict in the region."[105] Collectively, these conditions are not promising and suggest the United States will have less influence over Pakistan during future crises.[106]

In stark contrast to the progressively declining U.S. relationship with Pakistan, China enjoys relatively close ties to Pakistan—a relationship that is only growing stronger. Pakistan considers Beijing an "all-weather friend" and a reliable strategic partner both economically and militarily.[107] This sentiment is ironic, as China is just as concerned as the United States about the potential for a nuclear war in South Asia and would actively seek to avoid such an outcome to preserve its regional economic stakes.[108] Beijing has invested heavily in Pakistan to include assistance with its civilian nuclear power plants, infrastructure improvement projects, construction of Gwadar Port, and most notably its $55 billion investment in the China-Pakistan Economic Corridor that will link Chinese imports/exports to the Arabian Sea.[109] China also played a crucial role in the progression of Pakistan's nuclear ambitions as Beijing provided delivery vehicles and assisted in enhancing Islamabad's indigenous missile and fissile material production capabilities.[110] Of course, there is also the obvious common ground of seeking to curb India's expanding regional influence and economic growth, making Pakistan an ideal partner and a strategic hedge against New Delhi. The aforementioned dynamics, coupled with already deep historical ties, will make China a more feasible third-party broker with Pakistan during future crises.

The evolving geopolitical landscape and the progressive realignment of traditional patron relationships in the region may mandate a different strategy and suggest that a quadrilateral approach may be a more appropriate response to future South Asian crises. China's strong influence with Pakistan and its desire to prevent a potential escalation that risks nuclear war make Beijing a viable broker for Islamabad. Conversely, growing U.S. relations with India may be leveraged effectively to represent a viable third-party broker for India. In this light, a four-party de-escalation process could prove to be a feasible method of international intervention in the future. Splitting up the responsibilities of crisis monitoring, in extremis bilateral intelligence-sharing channels could potentially be preestablished between the United States and China to address the rapid de-escalation requirements that will be inherent to the introduction of LYNWs. While not an ideal situation, as there are trust barriers between Beijing and Washington, the sharing of sanitized information in a

Indian army's BrahMos Mobile Autonomous Launchers, February 7, 2014 (Courtesy Anirvan Shukla)

timely manner is certainly better than the alternative of idly watching a rapid and uncontrolled escalation unfold. Preemptive formation of intervention delegation parties by the United States and China with rough outlines of prepared material to aid in the mediation process may also be effective. This could be a more comprehensive version of the "notional playbook" the United States utilized during the Mumbai crisis, which had been developed during the previous two India-Pakistan crises since declared nuclearization.[111]

Opportunities

Despite a negative trajectory toward the revival of LYNWs within the nuclear domain, there are avenues the international community could explore to address South Asian issues.[112] The opportunities should come from the broader international community, not the United States specifically, due to the fact that U.S. credibility with Pakistan has waned as Washington has placed its burgeoning relationship with New Delhi on full display.[113] Perceptions of preferential treatment by the United States toward India render it a biased broker in the Pakistani view. As such, other players on the international stage should be encouraged to take more proactive roles in the process to defuse tensions in South Asia. These include obvious players such as China, who shares a strong patron relationship with Pakistan, as well as other regional actors such as Sri Lanka, Bangladesh, and Nepal, who also have much to lose in the event of a nuclear escalation. Russia is another possibility, as Moscow shares historic defense ties with India and a growing relationship with Pakistan.[114] Under these premises, two opportunities are presented for consideration: steering Pakistan toward a safer employment of LYNWs through international collaboration on training, education, and lessons learned, and establishing a viable international mediation forum for India and Pakistan to address enduring bilateral issues such as the Kashmir issue, water-sharing agreements, and cross-border violence.

The window to dissuade Pakistan away from the prospect of LYNWs has already closed. A U.S. or international rebuke now would be deemed hypocritical and dismissed by the Pakistanis, given Washington's recent reconsideration of LYNWs. However, symposiums and other discussions with Islamabad about the intricacies of the LYNW experience in Europe may help Islamabad shape its decisions regarding LYNW architecture in a constructive and informed manner. This is already occurring to some extent through multitrack talks, but these efforts should be expanded.[115] This may address some of the issues of Pakistan walking away with the wrong endstates and lessons learned about LYNWs in Europe based upon a limited consumption of Western nuclear scholarship.[116] These discussions should occur in a coalition-based setting and include not only the nuclear-armed nations, but also countries in Europe that house elements of the North Atlantic Treaty Organization's nuclear contingent, as these countries offer unique perspectives, particularly regarding the downsides of such systems.[117]

The United States and the larger international community have been reticent to officially acknowledge standing territorial issues between India and Pakistan as anything more than bilateral in nature—ironically, this is probably the most consistent U.S. policy position in South Asia. It is exceedingly clear, though, that bilateral mediation efforts have failed, and the numerous deep-seated issues between the two countries will require international mediation for any meaningful progress to occur. If South Asia represents the most likely environment for a nuclear war, then it stands to reason that the most effective way to prevent such an outcome is to address the core friction points that would incite a nuclear confrontation. Establishing an international forum for Pakistan and India to address their concerns accomplishes two things: it grants international legitimacy to these issues, and it provides a venue to vent during periods of heightened tensions. This could potentially provide a valuable de-escalation during a crisis, giving both sides the ability to pause and voice issues in the international courts rather than depending on international intervention to bring them back from the precipice. Previous crises since declared nuclearization (the Kargil crisis in 1999, the 2001–2002 Operation *Parakram* crisis, and the Mumbai terror attacks in 2008) demonstrated that established routes of bilateral de-escalation through hotlines are only effective to a point, and that both sides have habitually abandoned military and diplomatic dialogue when the stakes are at their highest.

Conclusion

The enormous challenges in South Asia represent wicked problems on the international stage with no easy or clear solution in sight. These challenges are complicated by waning U.S. influence with Pakistan and the increasingly complex regional dynamics that will demand multinational mediation approaches that include other powers such as China and perhaps Russia. The introduction of LYNWs to an already extremely tense environment will undoubtedly create great consternation among the various global powers and regional actors, but the nuclear restraint that binds together the nuclear-armed powers of the world has continued to hold despite crises, accidents, and miscalculations.[118] The great South Asian nuclear rivalry between Pakistan and India has produced several close calls. Both states, however, have navigated these crises without resorting to nuclear war, albeit with outside mediation assistance.[119] Despite numerous provocations, India has exercised strategic restraint, and Pakistan, whether purposefully or accidentally, has avoided pushing the envelope too far. These factors would lead nuclear optimists to conclude that both countries have developed enough of a sense of one another to sufficiently weather a storm of escalation.

In the absence of quantitative or qualitative conventional parity, which in all likelihood will never come irrespective of Islamabad's monetary commitments, military acquisitions, or modernization efforts, it is unsurprising that Pakistan turned to its nuclear arsenal to safeguard its sovereignty. While there is certainly cause for concern regarding the prospect of nuclear war in South Asia, particularly with the introduction of LYNWs, the situation is not without hope. Encouraging further Pakistani and Indian compliance with nuclear norms, creating constructive opportunities to address major friction points, and forming a supportive international community will go a long way toward defusing future tensions. JFQ

Notes

[1] Gurmeet Kanwal, *Sharpening the Arsenal: India's Evolving Nuclear Deterrence Policy* (New York: HarperCollins, 2017), 86–89.

[2] Mark Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers* (New York: Routledge Taylor and Francis Group, 2014), 16–17.

[3] Ibid., 159–164.

[4] Inderjit Panjrath, *Pakistan's Tactical Nuclear Weapons: Giving the Devil More Than His Due* (New Delhi: Vij Books, 2018), 19; Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton: Princeton University Press, 2014), 81; Bhumitra Chakma, *Pakistan's Nuclear Weapons* (New York: Routledge Taylor and Francis Group, 2009), 52.

[5] Tom Nichols, Douglas Stuart, and Jeffrey McCausland, eds., *Tactical Nuclear Weapons and NATO* (Carlisle Barracks, PA: Strategic Studies Institute, 2012), viii–ix.

[6] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 5, 18.

[7] Chakma, *Pakistan's Nuclear Weapons*, 48.

[8] Ibid., 40.

[9] Kanwal, *Sharpening the Arsenal*, 16.

[10] Chakma, *Pakistan's Tactical Nuclear Weapons*, 47.

[11] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 51; Chakma, *Pakistan's Nuclear Weapons*, 79.

[12] Chakma, *Pakistan's Nuclear Weapons*, 46.

[13] Ibid., 51.

[14] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 34*;* Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 92; Sadia Tasleem and Tony Dalton, "Nuclear Emulation: Pakistan's Nuclear Trajectory," *The Washington Quarterly* 41, no. 4 (Winter 2019), 138.

[15] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 22–24, 71–73; V.N. Veda, *Pakistan's Nuclear Weapons* (New Delhi: KW Publishers, 2012), 25.

[16] Kanwal, *Sharpening the Arsenal*, 50.

[17] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 85.

[18] Chakma, *Pakistan's Nuclear Weapons*, 56.

[19] Narang, *Nuclear Strategy in the Modern Era*, 55.

[20] Ibid., 56.

[21] Chakma, *Pakistan's Nuclear Weapons*, 60.

[22] Narang, *Nuclear Strategy in the Modern Era*, 86–87; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 26; Panjrath, *Pakistan's Tactical Nuclear Weapons*, 44–45.

[23] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 90.

[24] Ashley J. Tellis, *India's Emerging Nuclear Posture: Between Recessed Deterrent and Ready Arsenal* (Santa Monica, CA: RAND, 2001), 251.

[25] Ibid.

[26] Ibid., 252–253.

[27] Ibid., 253.

[28] Ibid., 254.

[29] Narang, *Nuclear Strategy in the Modern Era*, 100.

[30] Ibid.

[31] Tellis, *India's Emerging Nuclear Posture*, 302.

[32] Ibid., 374–378.

[33] Chakma, *Pakistan's Nuclear Weapons*, 49.

[34] Tellis, *India's Emerging Nuclear Posture*, 312–313.

[35] Ibid., 321.

[36] Ibid., 342–344.

[37] Ibid., 342.

[38] Ibid., 347.

[39] Narang, *Nuclear Strategy in the Modern Era*, 95.

[40] Ibid., 94–95.

[41] Jeffrey Larsen and Kerry Kartchner, *On Limited Nuclear War in the 21st Century* (Palo Alto: Stanford University Press, 2014), 107; David O. Smith, *The U.S. Experience with Tactical Nuclear Weapons: Lessons for South Asia* (Washington, DC: The Stimson Center, March 4, 2013), 4.

[42] Moeed Yusuf, *Brokering Peace in Nuclear Environments* (Palo Alto: Stanford University Press, 2018), 158.

[43] Ibid., 171; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 65.

[44] Larsen and Kartchner, *On Limited Nuclear War in the 21st Century*, 107; Tasleem and Dalton, "Nuclear Emulation," 140–141; Meenakshi Sood, "Pakistan's Response to Cold Start Doctrine," *Centre for Land Warfare Studies* 94 (March 2017), 1–3.

[45] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 44.

[46] Smith, *The U.S. Experience with Tactical Nuclear Weapons*, 4.

[47] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 119, 124–125; Narang, *Nuclear Strategy in the Modern Era*, 86–87.

[48] Narang, *Nuclear Strategy in the Modern Era*, 86–87.

[49] Scott Sagan and Kenneth Waltz, *The Spread of Nuclear Weapons: An Enduring Debate* (New York: Norton, 2013), 2.

[50] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 5.

[51] Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (New York: Cambridge University Press, 2017), 121.

[52] Larsen and Kartchner, *On Limited Nuclear War in the 21st Century*, 108; Sechser and Fuhrmann, *Nuclear Weapons and Coercive Diplomacy*, 149.

[53] Kanwal, *Sharpening the Arsenal*, 17–25.

[54] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 37; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 86; Kanwal, *Sharpening the Arsenal*, 31.

[55] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 77.

[56] V. Sahay, *Tactical Nuclear Weapons Deterrence Stability Between India and Pakistan* (New Delhi: Gaurav Book Centre, 2018), 12–23; Kanwal, *Sharpening the Arsenal*, 123–132.

[57] Narang, *Nuclear Strategy in the Modern Era*, 103–104.

[58] Kanwal, *Sharpening the Arsenal*, 10, 32.

[59] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 47–48.

[60] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 34; Panjrath, *Pakistan's Tactical Nuclear Weapons*, 47–48.

[61] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers,* 34; Panjrath, *Pakistan's Tactical Nuclear Weapons*, 46.

[62] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 49.

[63] Ibid., 61.

[64] Kanwal, *Sharpening the Arsenal*, 13; Sechser and Fuhrmann, *Nuclear Weapons and Coercive Diplomacy*, 36, 150.

[65] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 49.

[66] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 61.

[67] Kanwal, *Sharpening the Arsenal*, 32.

[68] Smith, *The U.S. Experience with Tactical Nuclear Weapons*, 8–10.

[69] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 46–49; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 34.

[70] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 46–49; Narang, *Nuclear Strategy in the Modern Era*, 86–87; Chakma, *Pakistan's Nuclear Weapons*, 78.

[71] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 61.

[72] Kanwal, *Sharpening the Arsenal*, 7, 50; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 75.

[73] Kanwal, *Sharpening the Arsenal*, 13, 17, 25.

[74] Narang, *Nuclear Strategy in the Modern Era*, 111.

[75] Smith, *The U.S. Experience with Tactical Nuclear Weapons*, 10.

[76] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 26, 84–85.

[77] Kanwal, *Sharpening the Arsenal*, 17.

[78] Sannia Abdullah, "Nuclear Ethics? Why Pakistan Has Not Used Nuclear Weapons . . . Yet," *The Washington Quarterly* 41, no. 4 (Winter 2019), 159.

[79] Tasleem and Dalton, "Nuclear Emulation," 150.

[80] Eric Schlosser, *Command and Control* (New York: Penguin, 2013), 174.

[81] Narang, *Nuclear Strategy in the Modern Era*, 85.

[82] Smith, *The U.S. Experience with Tactical Nuclear Weapons*, 40.

[83] Ibid., 44.

[84] Veda, *Pakistan's Nuclear Weapons*, 49, 60, 70; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 126, 132.

[85] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 89.

[86] Chakma, *Pakistan's Nuclear Weapons*, 79; Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 85, 89.

[87] Sood, "Pakistan's Response to Cold Start Doctrine," 2.

[88] Larsen and Kartchner, *On Limited Nuclear War in the 21st Century*, 107; Tasleem and Dalton, "Nuclear Emulation," 140–141; Sood, "Pakistan's Response to Cold Start Doctrine," 1–3.

[89] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 80.

[90] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 5, 18.

[91] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 81; Panjrath, *Pakistan's Tactical Nuclear Weapons*, 21.

[92] Yusuf, *Brokering Peace in Nuclear Environments*, 178–179.

[93] Ibid., 23.

[94] Ibid., 158.

[95] Ibid.

[96] Ibid., 28.

[97] Ibid., 40–41.

[98] Ibid., 40.

[99] Ibid., 42.

[100] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 26; Sood, "Pakistan's Response to Cold Start Doctrine," 6.

[101] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 26; Narang, *Nuclear Strategy in the Modern Era*, 108–109.

[102] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 71; Kanwal, *Sharpening the Arsenal*, 32.

[103] Veda, *Pakistan's Nuclear Weapons*, 50.

[104] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 72.

[105] Ibid.

[106] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 66.

[107] Veda, *Pakistan's Nuclear Weapons*, 2.

[108] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 71.

[109] Ibid., 71–74.

[110] Veda, *Pakistan's Nuclear Weapons*, 2, 35; Chakma, *Pakistan's Nuclear Weapons*, 28.

[111] Yusuf, *Brokering Peace in Nuclear Environments*, 140.

[112] Amy F. Woolf, *Nonstrategic Nuclear Weapons*, RL32572 (Washington, DC: Congressional Research Service, 2017), 1–2.

[113] Panjrath, *Pakistan's Tactical Nuclear Weapons*, 72.

[114] Ibid., 75.

[115] Fitzpatrick, *Overcoming Pakistan's Nuclear Dangers*, 66.

[116] Tasleem and Dalton, "Nuclear Emulation," 143.

[117] Smith, *The U.S. Experience with Tactical Nuclear Weapons*, 9–10.

[118] Abdullah, "Nuclear Ethics?" 158.

[119] Yusuf, *Brokering Peace in Nuclear Environments*, 24.

Annual air combat tactics, humanitarian assistance, and disaster relief exercise Cope North increases readiness and interoperability of U.S. Air Force, Japan Air Self-Defense Force, and Royal Australian Air Force (U.S. Air Force/ Matthew Bruch)

The Second Island Cloud

A Deeper and Broader Concept for American Presence in the Pacific Islands

By Andrew Rhodes

In the early 20th century, the visionary Marine officer Earl "Pete" Ellis compiled remarkable studies of islands in the Western Pacific and considered the practical means for the seizure or defense of advanced bases. A century after Ellis's work, China presents new strategic and operational challenges to the U.S. position in Asia, and it is time for Washington to develop a coherent strategy, one that will last another 100 years, for the islands of the Western Pacific. It has become common to consider the *second island chain* as a defining feature of Pacific geography, but when Ellis mastered its geography, he saw not a "chain," but a "cloud." He wrote in 1921 that the "Marshall, Caroline, and Pelew Islands form a 'cloud' of islands stretching east and west." His apt description of these archipelagoes serves well for a broader conception of the islands in, and adjacent to, traditional definitions of the second island chain. A new U.S. strategy should abandon the narrow lens of the "chain" and emphasize a broader

Andrew Rhodes wrote this essay while a student at the U.S. Naval War College. It won the Strategic Research Paper category of the 2019 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

second island cloud that highlights the U.S. regional role and invests in a resilient, distributed, and enduring presence in the Pacific.

The United States has often been of two minds about its role in Asia, and recent heated debate on the future of U.S. security commitments in the region is no exception. This pendulum has swung before, from the heavy presence lasting from World War II through Vietnam to a partial retrenchment under Richard Nixon's Guam Doctrine, and back toward statements of a greater strategic emphasis on the region under the Obama administration's "Rebalance to Asia."[1] Despite some inconsistent messaging on military alliances and trade relationships, the Trump administration has indicated a major focus on Asia in the 2018 National Defense Strategy (NDS) and its strategy for a "Free and Open Indo-Pacific."[2] Regardless of whether the United States pursues broad engagement with the region, focuses on military containment of China, or decides to allow a larger Chinese sphere of influence in the Western Pacific, the second island cloud represents critical geography for what Vice President Mike Pence has called an "ironclad commitment" to the region.[3] To demonstrate this commitment and respond to operational imperatives, there is a compelling need to get serious about the second island cloud—we need to identify the challenges to a sustained or enhanced U.S. presence and to pursue near-term opportunities that advance U.S. national interests. A strategy for the second island cloud should deepen the unique U.S. relationship with these islands and reframe the strategic discussion with a broader definition that includes valuable islands excluded from the second island chain.

Origins and Interpretations

The second island chain has no official standing among geographers or international organizations but has served as shorthand for the line of islands extending from the Japanese mainland, through the Nanpõ Shotõ, the Marianas, and the western Caroline Islands, before terminating somewhere in eastern Indonesia. The second island chain lies to the east; the *first island chain*, which is also imprecise, generally comprises a line from southern Japan through the Ryukyus and Taiwan, terminating in the Philippines or Borneo. The island chains took on strategic importance for the United States when it annexed the Philippines and Guam after the Spanish-American War. The fortification of these outposts was a central feature of negotiations in the 1920s that vainly sought to prevent military competition and conflict between the United States and Japan. Michael Green notes that as much as many planners of the interwar period regretted the decision not to establish robust fortifications of strategic points such as Guam, the restrictions of the Washington Naval Treaties incentivized key innovations in fleet mobility, such as underway replenishment, to mitigate against the threat to fixed fueling points.[4]

The notorious geopolitician Karl Haushofer was one of the first to describe the island chain concept, calling them "offshore island arcs."[5] Haushofer served as German military attaché in Tokyo before he established his Institute for Geopolitics at the University of Munich and gained influence in the 1930s with Nazi leaders such as Adolf Hitler and Rudolf Hess. Leading architects of the post–World War II Pacific security architecture, including Douglas MacArthur and Dean Acheson, also invoked the island chains. Chinese strategists have focused contemporary attention on the island chains, and it is Chinese adaptations and descriptions of the island chains that have reintroduced the concept to American strategists.[6] Throughout the remarkable modernization of China's military since the 1990s, its leaders have emphasized the military challenge of U.S. and allied deployments in the island chains and the strategic importance of the waters they enclose.[7] A central figure in the promulgation of the island chains in Chinese geostrategy and military planning was Admiral Liu Huaqing, often referred to as the "Father of the People's Liberation Army Navy," who served as its commander in the 1980s and then as vice chairman of the Central Military Commission in the 1990s. One leading Chinese scholar on seapower references control over the Pacific islands as key to U.S.-led efforts to "contain China," invokes the operational imperative to "break through" the island chains, and also highlights the power of small islands to confer broad "jurisdictional sea area."[8] Andrew Erickson and Joel Wuthnow catalog these discussions of the island chains concept in Chinese sources and lay out three ways that Chinese authors have thought about island chains: as *barriers*, *springboards*, and *benchmarks*.[9] These three concepts provide a useful framework for not only understanding Chinese perspectives but also analyzing U.S. interests in the region. A durable U.S. regional strategy should reject what have become Chinese concepts of the islands and redefine the geography as a cloud, then consider the various roles of the second island cloud as a barrier, springboard, and benchmark.

These three perspectives are already inherent in some of the debates on U.S. relationships and force posture in the Western Pacific. The argument for "archipelagic defense" typifies the barrier concept, seeking new ways to defend the island chains in the face of daunting Chinese capabilities.[10] The second island chain has served as a springboard for the U.S. military for decades, launching strategic bomber strikes at the end of World War II and in Vietnam, and sustaining the Continuous Bomber Presence Mission from Guam's Andersen Air Force Base since 2004.[11] Homeporting submarines at Guam and redeployment of Okinawa-based Marines to the island have enhanced the springboard aspect of one link in the second island chain.[12] Finally, the second island chain has been an important benchmark of China's growing maritime power, both for those seeking to balance against Chinese expansionism and those advocating a more conciliatory approach to China. Lyle Goldstein, for example, argues that a reduction of U.S. forces on Guam would foster trust and greater cooperation with China.[13] Goldstein also employed the benchmark concept to note Chinese focus on the Philippine Sea—between the two island chains—as nascent evidence of an "evolving new multipolarity."[14]

Island Geography

The second island cloud lies to the east of the first island chain, across the Philippine Sea. This cloud spans a complicated patchwork of sovereignty arrangements, political contexts, and economic challenges. The concept of a second island cloud should build on three basic types of islands in the traditional *chain* definition: Japanese and Indonesian territory at the northern and southern ends, a core of U.S. territory in the Marianas, and the island groups adjacent to the core consisting of the Republic of Palau and portions of the Federated States of Micronesia (FSM). The second island cloud should also include the islands in the Carolines that make up the rest of the FSM, the Republic of the Marshall Islands (RMI), and islands on the southern rim of the Caroline Basin belonging to Indonesia and Papua New Guinea.

The fully sovereign foreign territory at the northern and southern anchors of the second island cloud is markedly different in terms of U.S. security architecture. The Nanpõ Shotõ are covered under existing U.S.-Japan treaties, and U.S. forces enjoy access to military facilities, such as the airfield at Iwo Jima.[15] Indonesia, which governs the islands along the southern rim of the Caroline Basin, remains a nascent security partner for the United States, and U.S. forces have enjoyed only limited access to the economically challenged parts of eastern Indonesia. Papua New Guinea, whose islands mark the southeastern rim of the Caroline Basin, is an even more nascent partner for the United States, although the joint U.S.-Australia initiative at Manus Island, announced by Pence in 2018, is an important development for an area not included in the second island chain.

Discussions of Pacific strategy regularly reference the U.S. territories in the Marianas, but these islands are poorly understood. Guam and the Commonwealth of the Marianas Islands (CNMI) have subtly different statuses in U.S. law, and each has a non-voting representative in Congress. Both Guam and the CNMI are unincorporated territories where the Constitution applies only partially. Both territories have a non-voting member of the House of Representatives, but there are subtle differences in the application of Federal law in each territory. Guam is the largest, most populous, and most developed island in the Marianas and hosts a substantial U.S. military presence, while the CNMI—including the smaller and less populous islands of Saipan, Tinian, and Rota—hosts only small-scale U.S. military training. The CNMI has struggled economically in the last decade and has started to rely for jobs and growth on Chinese investment in casino tourism, an alarming development for those who advocate for the CNMI's importance to U.S. regional military strategy.[16]

Palau and the western end of FSM are links in the traditional chain, but these islands are part of a broader geography and have a uniquely complicated relationship with the United States. The shared history and similar political status of Palau, the FSM, and the RMI make it imperative to consider all three of these island nations together and highlight a key dimension of why the more expansive second island cloud is more coherent and accurate than the chain. The United States administered these islands as the Trust Territory of the Pacific Islands following World War II and then devolved sovereignty to the three independent governments under Compacts of Free Association (CFA).The CFAs with the FSM and the RMI entered into force in the 1980s and were revised in 2003, while the CFA with Palau entered into force in 1994, and a long-pending revision entered into force in late 2018.

These three sovereign nations, known collectively as the Freely Associated States (FAS), receive various forms of financial assistance and public services from the U.S. Government, and FAS citizens may live and work in the United States, including serving in the military. The U.S. Government takes full responsibility for the defense of FAS territory and enjoys exclusive rights to establish and control access to military facilities in the islands. All three nations face development challenges relating to their remote locations and undiversified economies and have seen heavy outward migration, with nearly a quarter of FAS citizens living in the United States.[17] Palau has much higher per capita gross domestic product and has been more successful at investing U.S. assistance than its neighbors. The economic outlook is more discouraging for the FMS and RMI as a 2024 deadline looms for both nations to transition away from direct U.S. support in favor of disbursements from a trust fund established in 2003.[18] The trust fund sought to place the FMS and RMI on a more stable long-term financial footing; however, enduring structural challenges, weak performance, and corruption suggest poor prospects for a successful transition to trust fund income.[19]

Barrier and Springboard: The Military Potential of the Second Island Cloud

The second island cloud can play a vital role in concepts in the 2018 NDS Global Operating Model, filling operational space for the "contact layer" and enabling maneuver for the "blunt layer."[20] While Ellis and the "War Plan Orange" generation sought protected anchorages for the fleet, since 1942 the military value of these islands has resided primarily in airfields, even as growing Chinese capabilities for long-range strike make them increasingly vulnerable.[21]

Active defenses, like missile interceptors, and passive defenses, such as hardening, play a central role in mitigating long-range fires, but the chief defensive contribution that the second island cloud can offer is dispersal.[22] Dispersal bases are in short supply in the Pacific, but the second island cloud includes several of the "secondary and tertiary operating locations" called for by Elbridge Colby, the principal architect of the 2018 NDS.[23] The importance of Palau and Yap, from which aircraft can range the Philippine Sea, is evident, but the eastern Carolines also have utility. The FSM's Chuuk, for example, is several

U.S. Air Force and Japan Air Self-Defense Force conduct Cope North annually at Andersen Air Force Base, Guam, to increase combat readiness and interoperability, concentrating on coordination and evaluation of air tactics, techniques, and procedures, February 21, 2011 (U.S. Air Force/Angelita M. Lawrence)

hundred kilometers closer to Taipei than Darwin, Australia. Operational discussions do not typically include the RMI, but the Marshalls and Aleutians are equidistant from potential combat zones; Kwajalein and Attu are each roughly 2,900 miles from Okinawa.

The second island cloud's military potential could grow with the introduction of new capabilities and operational concepts. U.S. withdrawal from the Intermediate-Range Nuclear Forces Treaty could lead to the deployment of mobile intermediate-range missiles in the second island cloud that could range key regional targets and complicate adversary targeting.[24] Secondary airfields in the second island cloud could also prove valuable to supporting operations by future "arsenal planes" with large loadouts of standoff weapons, an old concept that gained new energy through a 2016 Strategic Capabilities Office program.[25] A growing body of operational literature on new concepts for combat logistics in the Pacific has developed recently, some of it hearkening back to World War II and the anchorages surveyed by the likes of Ellis.[26] Expeditionary "forward arming and refueling points" at tertiary airports offer the potential of much more dynamic airpower, particularly with aircraft capable of operating from austere facilities.[27] The ability to rearm combatants, and potentially even submarines from support ships in sheltered anchorages, rather than pierside at established bases, offers a new take on an old concept to regenerate naval combat power despite the Western Pacific threat environment.[28] All these concepts are directly compatible with the second island cloud concept and would benefit from peacetime infrastructure investment throughout the islands.[29]

Demonstrating Regional Staying Power Through the Second Island Cloud

Sustaining and growing the U.S. presence in the second island cloud is important for the springboard or barrier purposes; it would also provide an important benchmark demonstrating to rivals, allies, and partners alike that the United States intends to sustain its role as a Pacific power. The United States should integrate the second island cloud into what Jakub Grygiel and Wess Mitchell call "tighter frontline webs" of security relationships.[30] The means to strengthen these ties in the second island cloud are primarily nonmilitary and suggest a greater focus on diplomatic, political, and development aspects of U.S. relationships with these islands. Traditional security cooperation with Indonesia and Japan helps ensure the northern anchor remains secure and U.S. access grows along the southern edge of the second island cloud, although there is room to improve synchronization with other instruments of national power.[31]

Washington should also reinforce its commitment to its territories in the Marianas where foreign and domestic policy overlap. Both Guam and the CNMI would benefit from enhanced

Two U.S. Air Force B-1B Lancers assigned to 9th Expeditionary Bomb Squadron, deployed from Dyess Air Force Base, Texas, fly 10-hour mission from Guam through South China Sea, operating with USS *Sterett*, June 8, 2017 (U.S. Air Force/Richard P. Ebensberger)

commitments at the Federal level to support sustainable economic growth and address labor shortfalls while creating alternatives to potentially problematic Chinese investment.[32] The Department of Interior–led Interagency Group on Insular Areas was established in 2010 to make recommendations on Federal programs in Guam, American Samoa, the U.S. Virgin Islands, and the CNMI.[33] The group could play a role in coordinating long-term U.S. policy for the second island cloud, but would be more effective with more frequent meetings and the inclusion of additional agencies at the assistant secretary level. Enhancing the influence of Guam and the CNMI in Congress, potentially through greater staff support on their representatives' assigned committees, would also build capacity for shaping legislation that supports these islands. Although a near impossibility in the current political climate, statehood for a unified Guam and the CNMI could imitate Hawaii's economic success and provide an unmistakable symbol of long-term U.S. commitment to regional presence.

Senior-level visits are an important currency in diplomacy, particularly with partners like the FAS that get less attention. In 2018, senior Defense officials, including the Under Secretary of the Navy and the Assistant Secretary of Defense for Asian and Pacific Security Affairs, visited underappreciated parts of the second island cloud.[34] High-level officials from Washington should sustain a regular calendar of bilateral and multilateral meetings to discuss diplomatic, defense, and development initiatives in venues like the Pacific Islands Forum.[35]

Investing in the economic development of the FAS entails serious challenges but supporting the long-term stability of these U.S.-aligned nations offers a high potential return for the United States. These nations already rely on assistance from multilateral financial institutions such as the Asian Development Bank (ADB), and their economic situation leaves them vulnerable to bilateral economic inducements from rivals probing for weakness in the U.S. regional position. ADB assistance to the FAS is small by the standards of most international development programs but is significant in small economies like those of the FAS. ADB assistance in 2017 was $8.3 million to the FSM, $10.5 million to the RMI, and less than $1 million to Palau.[36] In the larger context of regional relationships, it is important to note that Palau and the RMI are among the few nations that maintain diplomatic relations with Taiwan, making them a target for

Terminal High Altitude Area Defense interceptor missile launches from Meck Island to intercept ballistic missile target during Missile Defense Agency integrated flight test, Republic of the Marshall Islands, October 25, 2012 (U.S. Navy)

Chinese coercive diplomatic efforts.[37] Deliberate erosion of FAS support for the United States by a challenger with deep pockets could introduce substantial friction should the United States seek expanded presence or new facilities.

A new focus on economic development that complements the RMI and FSM trust funds but endures beyond them could increase investment in infrastructure and such key industries as tourism and fisheries to build a stronger economic foundation. Revenue from fishing licenses has been a critical source of foreign exchange for the FAS with their large exclusive economic zones but small economic bases. The ADB notes that in 2017, revenue from fishing licenses was the primary factor returning the economy of the FSM to growth after a period of contraction.[38] Monitoring and oversight are essential to effective development programs, but the strategic imperatives suggest the United States should accept the risk of some inefficiency in an expanded aid program while continuing to address structural economic reform and corruption. The U.S. Agency for International Development (USAID) plays only a minor role in the second island cloud, as all assistance is managed through the CFA, but it has been active in disaster preparedness in the FSM.[39] Washington should make greater use of USAID, which has expertise and mechanisms for providing the needed support while managing the tradeoffs between efficiency and foreign policy objectives, in the FAS.

Finally, just as Japan is the linchpin of the northern part of the region, Australia plays a critical role throughout the South Pacific, both as a staunch U.S. ally and as a leading voice in venues such as the Pacific Islands Forum.[40] The United States should seek additional opportunities, such as that recently announced for Manus Island, to partner with Australia in new defense, diplomacy, and development efforts across Oceania. India's growing engagement in the region also offers the possibility of coordinating on second island cloud investment within the emerging Quadrilateral Security Dialogue with Japan, Australia, and India.[41]

Counterarguments

There are strategic, financial, political, and operational arguments against a deeper U.S. commitment to the region. At the strategic level, some might argue that an enhanced U.S. focus and posture in the area will contribute to a security dilemma and further incentivize China's military buildup and aggressive behavior. Replacing or augmenting the RMI and FSM trust funds with additional financial support, as with any development program, risks open-ended dependence of small economies on the U.S. Government. Politically, enhancing military presence in territories where the population is not composed of U.S. citizens or does not enjoy the full benefits of citizenship could contribute to a narrative of the United States as an exploitative neocolonial power. Operationally, as much as the airfields of the second island cloud allow for greater dispersal of forces and would complicate adversary targeting, the facilities are small, fixed, and difficult to defend in the face of large numbers of long-range weapons. Aircraft scattered among the islands might survive but could quickly exhaust fuel supplies and might not find any means to rearm.

This article is not the first to argue for a reconception of the second island chain, and some might argue that the second island cloud is still too narrow. Former Pacific Fleet Commander Admiral Scott Swift suggested in 2018 that the second island chain circles around New Guinea, then crosses the Indian Ocean through Diego Garcia and terminates at Djibouti.[42]

Conclusion

A stable footing in the second island cloud is worth these costs and risks, as it can serve as a strategic position and powerful symbol that transcends the operational imperatives to balance Chinese military capabilities in the near term. In the first 50 years after the United States took possession of Guam, Ellis saw the rise of Japan and envisioned key geographic aspects of its defeat that took place two decades after his death. In 1942, geostrategist Nichols Spykman foresaw that technological change and political shifts could one day make Chinese airpower more dominant than British, Japanese, or American seapower in what he called the "Asian Mediterranean."[43] In only 30 years, China changed from a strategic partner in the Cold War to a peer rival in a newly bipolar world. China is pursuing a much more expansive role on the international stage with new security relationships and overseas bases and is even contemplating military alliances.[44] The coming decades will see major structural changes to the international system, and a truly long-term strategy should secure America's Pacific position through and beyond the current competition.

Ely Ratner argues that "it is imperative that the United States stop China's advances toward exerting exclusive and dominant control over key geographic regions."[45] With growing Chinese investment and influence throughout the Pacific islands, the second island cloud can play a central role in near-term efforts to avoid a power vacuum and create what Ratner calls "spheres of competition."[46] The current administration's Indo-Pacific strategy and the Asia Reassurance Initiative Act passed by Congress have brought important focus to the policy discussion on the region, but sustained energy is required to realize these ambitions.[47] In addition to developing new partnerships, Washington should double down where it is already strong—the second island cloud is squarely aligned to the United States, but U.S. policy must work hard to sustain that alignment and build on it to our advantage.

Ellis's description of an island cloud aptly captures the complexity and diversity of the key geography and provides a framework for lasting and dispersed strength—chains fail with a single weak link, but clouds are resilient. The argument for a durable commitment to the second island cloud in the 21st century is much the same as what Ellis wrote in 1913: "Once secure it will stand as a notice to all the world that America is in the Western Pacific to stay."[48] JFQ

Notes

[1] Michael J. Green, *By More Than Providence: Grand Strategy and American Power in the Asia Pacific Since 1783* (New York: Columbia University Press, 2017).

[2] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, January 2018); "Fact Sheet: Advancing a Free and Open Indo-Pacific Region," Department of State, November 18, 2018, available at <www.state.gov/advancing-a-free-and-open-indo-pacific-region/>.

[3] "Fact Sheet: Advancing a Free and Open Indo-Pacific Region."

[4] Green, *By More than Providence*, 141.

[5] Andrew S. Erickson and Joel Wuthnow, "Why Islands Still Matter in Asia," *The National Interest*, February 5, 2016, available at <https://nationalinterest.org/feature/why-islands-still-matter-asia-15121>.

[6] Andrew S. Erickson and Joel Wuthnow, "Barriers, Springboards, and Benchmarks: China Conceptualizes the Pacific 'Island Chains,'" *The China Quarterly* 225, no. 3 (2016), 1–22.

[7] Toshi Yoshihara and James R. Holmes, *Red Star Over the Pacific: China's Rise and the Challenge to U.S. Maritime Strategy*, 2nd ed. (Annapolis, MD: Naval Institute Press, 2018), 125–126.

[8] Hu Bo, "On China's Important Maritime Interests," *Asia-Pacific Security and Maritime Affairs* 3, 2015.

[9] Erickson and Wuthnow, "Barriers, Springboards, and Benchmarks."

[10] Andrew F. Krepinevich, Jr., "How to Deter China: The Case for Archipelagic Defense," *Foreign Affairs*, March/April 2015.

[11] John T. Correll, "Arc Light," *Air Force Magazine*, January 2009, 58–62; "Continuous Bomber Presence Mission," Andersen Air Force Base Web site, available at <www.andersen.af.mil/CBP/>.

[12] Shirley A. Kan, *Guam: U.S. Defense Deployments*, RS22570 (Washington, DC: Congressional Research Service, November 26, 2014), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a589626.pdf>.

[13] Lyle Goldstein, *Meeting China Halfway: How to Defuse the Emerging U.S.-China Rivalry* (Washington, DC: Georgetown University Press, 2015).

[14] Lyle Goldstein, "China's Naval Expansion Is No Threat," *The National Interest*, June 6, 2018, available at <https://nationalinterest.org/feature/chinas-naval-expansion-no-threat-26150>.

[15] Caitlin Dornbos, "After Years of Talks, Japan to Buy Island for U.S. Aircraft Carrier Landing Practice," *Stars and Stripes*, January 10, 2019.

[16] Grant Newsham, "Mariana Islands—U.S. Military Strategy 'On Hold,'" *East-West Center Asia Pacific Bulletin*, no. 415, March 26, 2018, available at <www.eastwestcenter.org/publications/mariana-islands-us-military-strategy-hold>.

[17] David Gootnick, *Compacts of Free Association: Issues Associated with Implementation in Palau, Micronesia, and the Marshall Islands*, GAO-16-550T (Washington, DC: Government Accountability Office [GAO], April 5, 2016), 33, available at <www.gao.gov/assets/680/676338.pdf>.

[18] *Compacts of Free Association: Actions Needed to Prepare for the Transition of Micronesia and the Marshall Islands to Trust Fund Income*, GAO-18-415 (Washington, DC: GAO, May 2018), available at <www.gao.gov/assets/700/691840.pdf>.

[19] Ibid.

[20] *Summary of the 2018 National Defense Strategy*; Elbridge Colby, *Hearing to Receive Testimony on China and Russia*, Testimony Before the Senate Armed Services Committee, video, 2:28:37, January 29, 2019, available at <www.armed-services.senate.gov/hearings/19-01-29-china-and-russia>.

[21] Edward Miller, *War Plan Orange: The U.S. Strategy to Defeat Japan, 1897–1945* (Annapolis, MD: Naval Institute Press, 2007); Mark Cozad and Nathan Beauchamp-Mustafaga, *People's Liberation Army Air Force Operations over Water: Maintaining Relevance in China's Changing Security Environment*, RR2057 (Santa Monica, CA: RAND, 2017), available at <www.rand.org/pubs/research_reports/RR2057.html>; and Eric Heginbotham et al., *Chinese Attacks on U.S. Air Bases in Asia: An Assessment of Relative Capabilities, 1996–2017*, RB9858/2 (Santa Monica, CA: RAND, 2015), available at <www.rand.org/pubs/research_briefs/RB9858z2.html>.

[22] Peter Lupo et al., "Building a Response in the Pacific," *The Military Engineer*, September–October 2017, 42–45; "House Okays Tinian Divert $51M," press release, Office of Representative Gregorio Sablan of the Commonwealth of the Marianas Islands, July 30, 2018.

[23] Colby, *Hearing to Receive Testimony on China and Russia*.

[24] Jacob Heim, *Missiles for Asia? The Need for Operational Analysis of U.S. Theater Ballistic Missiles in the Pacific*, RR945 (Santa Monica, CA: RAND, 2016), available at <www.rand.org/pubs/research_reports/RR945.html>.

[25] David Axe, "The U.S. Air Force's Master Plan to Outgun China," *The National Interest*, February 8, 2016, available at <https://nationalinterest.org/blog/the-buzz/the-us-air-forces-master-plan-outgun-china-15145>; Zalmay Khalilzad et al., *The United States and Asia: Toward a New U.S. Strategy and Force Posture*, MR1315 (Santa Monica, CA: RAND, 2001), 87–88, available at <www.rand.org/pubs/monograph_reports/MR1315.html>.

[26] Jose Gonzalez, "Sustainment of Expeditionary Forces in the Pacific Theater During the Second World War: The Development of the Advanced Base and Mobile Base Programs and Their Relevance Today" (master's thesis, U.S. Marine Corps Command and Staff College, 2013), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a601780.pdf>; Brian Lasley, "MPSRON 3 Delivers Aid to Northern Mariana Islands," Defense Visual Information Distribution System Web site, November 9, 2018, available at <https://www.dvidshub.net/news/299346/mpsron-3-delivers-aid-northern-mariana-islands>.

[27] Joseph Trevithick, "Glimpse of the Future? MC-130 Sets Up Forward Refueling Point for MQ-9 Reaper Drone," *War Zone*, February 14, 2018, available at <www.thedrive.com/the-war-zone/18502/glimpse-of-the-future-mc-130-sets-up-forward-refueling-point-for-mq-9-reaper-drone>; Robert C. Owen, "Distributed STOVL Operations and Air-Mobility Support: Addressing the Mismatch between Requirements and Capabilities," *Naval War College Review* 69, no. 4 (2016); Robert Davis, "Forward Arming and Refueling Points for Fighter Aircraft: Power Projection in an Anti-Access Environment," *Air and Space Power Journal* (September–October 2014), available at <www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-28_Issue-5/F-Davis.pdf>.

[28] Hunter Stires, "1941 Asiatic Fleet Offers Strategic Lessons," U.S. Naval Institute *Proceedings* 142, no. 8 (August 2016), 58–63; Michael E. Moore, "Sustaining Naval Surface Combatant Vertical Launch System Munitions During Joint Operations" (master's thesis, National Defense University, 2017), available at <www.dtic.mil/dtic/tr/fulltext/u2/1032180.pdf>.

[29] Matthew White, "UCT-2 Conducts Underwater Demolition to Improve Port Access," *Seabee Magazine*, September 18, 2018, available at <http://seabeemagazine.navylive.dodlive.mil/2018/09/18/uct-2-conducts-underwater-demolition-to-improve-port-access/>.

[30] Jakub Grygiel and A. Wess Mitchell, *The Unquiet Frontier: Rising Rivals, Vulnerable Allies, and the Crisis of American Power* (Princeton: Princeton University Press, 2016), 168.

[31] Tommy Ross, "Leveraging Security Cooperation as Military Strategy," *The Washington Quarterly* 39, no. 3 (Fall 2016).

[32] David Gootnick, *Commonwealth of the Northern Mariana Islands: Recent Economic Trends and Preliminary Observations on Workforce Data*, GAO-18-373T (Washington, DC: GAO, February 6, 2018), available at <www.gao.gov/assets/690/689935.pdf>.

[33] See Department of the Interior, Office of Insular Affairs Web site, "Interagency Group on Insular Areas," available at <www.doi.gov/oia/igia/index2>.

[34] Jim Garamone, "Navy Undersecretary Modly Shores Up Alliances in Oceania," *Defense.gov*, October 2, 2018, available at <https://dod.defense.gov/News/Article/Article/1651378/navy-undersecretary-modly-shores-up-alliances-in-oceana/>.

[35] "U.S. Delegation Attends the 30th Pacific Islands Forum," media note, Department of State, August 20, 2018, available at <www.state.gov/r/pa/prs/ps/2018/08/285231.htm>.

[36] "Asian Development Bank and the Federated States of Micronesia: Fact Sheet," April 2019, available at <www.adb.org/publications/federated-states-micronesia-fact-sheet>; "Asian Development Bank and the Marshall Islands: Fact Sheet," April 2018, available at <www.adb.org/publications/marshall-islands-fact-sheet>; "Asian Development Bank and Palau: Fact Sheet," available at <www.adb.org/publications/palau-fact-sheet>.

[37] Data on Chinese aid to the Federated States of Micronesia are documented by the Lowy Institute for International Policy, available at <https://chineseaidmap.lowyinstitute.org/>.

[38] See "Asian Development Bank and Federated States of Micronesia: Fact Sheet."

[39] See "Foreign Aid Explorer: Micronesia (Federated States)," U.S. Agency for International Development, available at <https://explorer.usaid.gov/cd/FSM>.

[40] "Australia Is Battling China for Influence in the Pacific," *The Economist*, January 19, 2019, available at <www.economist.com/asia/2019/01/19/australia-is-battling-china-for-influence-in-the-pacific>.

[41] Balaji Chandramohan, "India's Strategic Expansion in the Pacific Islands," *The Diplomat*, June 13, 2018, available at <https://thediplomat.com/2018/06/indias-strategic-expansion-in-the-pacific-islands/>.

[42] Admiral Swift presented the map at "The New China Challenge Conference," hosted by the U.S. Naval Institute in October 2018. The map was reproduced in Kevin Rudd, "Can China and the United States Avoid War?" U.S. Naval Institute *Proceedings* 144, no. 12 (2018), available at <www.usni.org/magazines/proceedings/2018-12/can-china-and-united-states-avoid-war>.

[43] Nicholas Spykman, *America's Strategy in World Politics* (New York: Harcourt, Brace and Co., 1942), 469.

[44] Huang Yufan, "Q and A: Yan Xuetong Urges China to Adopt a More Assertive Foreign Policy," *New York Times*, February 9, 2016; and "Yan Xuetong: "China Will Be a Superpower within 10 Years," *Chinascope*, November–December 2013.

[45] Ely Ratner, *Hearing to Receive Testimony on China and Russia*, Testimony Before the Senate Armed Services Committee, video, 2:28:37, January 29, 2019, available at <www.armed-services.senate.gov/hearings/19-01-29-china-and-russia>.

[46] "The Great Wharf: Australia Is Edgy about China's Growing Presence on Its Doorstep," *The Economist*, April 21, 2018, 48–49, available at <www.economist.com/asia/2018/04/20/australia-is-edgy-about-chinas-growing-presence-on-its-doorstep>.

[47] *Asia Reassurance Initiative Act of 2018*, Pub. L. No 115–409, 115th Cong., 2nd sess., December 31, 2018, available at <www.congress.gov/bill/115th-congress/senate-bill/2736>.

[48] F.H. Schofield and E.H. Ellis, *Report of the Naval War College Committee of Defense of Guam*, Part 1 (1913), 14. Original document held in the U.S. Naval War College Archives.

Marine with Special Purpose Marine Air-Ground Task Force—Crisis Response—Africa 19.2, Marine Forces Europe and Africa, evaluates Moroccan soldiers during culminating event at Tifnit, Morocco, July 25, 2019 (U.S. Marine Corps/Margaret Gale)

America First ≠ America Alone

Morocco as Exemplar for U.S. Counterterrorism Strategy

By James B. Cogbill

On October 4, 2018, Secretary of State Mike Pompeo announced the release of President Donald Trump's new National Strategy for Counterterrorism (NSCT), stating that "the President's strategy emphasizes the importance of diplomacy and the role of international partnerships in combating the terrorist threats we face."[1] The first page of the NSCT includes the statement "America First does not mean America alone," indicating the essential role of key international partners.[2] Morocco is such a partner. In the years since 9/11, Morocco has built an effective program for counterterrorism (CT) and countering violent extremism (CVE), leading U.S. Africa Command (USAFRICOM) to label Morocco "Africa's premier security exporter."[3] This article evaluates Morocco as a model for the NSCT objectives regarding partner-nation CT/CVE activities, while also noting where Morocco's efforts could be improved.

Colonel James B. Cogbill, USA, wrote this essay while attending the U.S. Army War College. It won the Strategy Article category of the 2019 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

Background

Morocco is a parliamentary constitutional monarchy in which King Mohammed VI retains ultimate power and authority. Following the 2011 Arab Spring protests, the king introduced a new constitution that increased the powers of parliament and permitted direct elections for regional councils. Despite this liberalization, the king still retains near-exclusive power over the military and religious and foreign affairs. The population is 99 percent Sunni Muslim, and the king derives religious legitimacy through his constitutionally enshrined title as Commander of the Faithful and by tracing his lineage to the Prophet Muhammad. During Mohammed VI's reign, the economy has experienced steady growth but still suffers from significant youth unemployment, especially in urban areas.[4]

Located in northwest Africa, Morocco represents a key gateway to Europe, the Middle East, and Africa. This also makes it a key hub for migration—mostly from Africa to Europe—which is a security concern for the European Union. Despite this concern, Morocco enjoys excellent relations with the international community. The U.S. diplomatic relationship with Morocco dates back to 1777, representing the longest unbroken relationship in U.S. history.[5] Separately, Morocco is a "major non–North Atlantic Treaty Organization ally" and a co-chair of the Global Counterterrorism Forum, and it has been a key military partner through its participation in the coalition to defeat the so-called Islamic State (IS) and by hosting multinational exercises including USAFRICOM's largest such exercise, African Lion.[6]

Morocco as a Model for NSCT Objectives

The NSCT is divided into six lines of effort (LOEs). Morocco's example as a model CT partner is recognizable in the LOEs "strengthen the counterterrorism abilities of international partners" and "counter terrorist radicalization and recruitment." Under the "strengthen abilities" LOE, the NSCT states that the United States will help "professionalize the military, law enforcement, judicial, intelligence, and security services . . . of key partners."[7] With the assistance of the U.S. Embassy in Rabat, Morocco is well on its way to accomplishing all of these goals.

In order to professionalize its military, Morocco has invested several hundred million dollars for modernization, purchasing U.S. F-16 fighter jets, M1A1 tanks, and helicopters.[8] As stated, Morocco participates in the coalition to defeat IS and committed its F-16s to combat operations in Syria and for anti-Houthi strikes in Yemen.[9] Morocco operates a field hospital in Jordan that has served more than 1.5 million Syrian refugees, and it also provided a field hospital in response to the 2014 Ebola outbreak in West Africa.[10] Additionally, Morocco participates in peacekeeping missions, with more than 1,500 peacekeepers deployed to the Central African Republic and Democratic Republic of the Congo.[11] Morocco's military conducts partnership-building and professionalization activities with sub-Saharan militaries and trains more than 1,000 foreign officers and noncommissioned officers annually in its military academies and technical schools.[12] Such activities are the reason USAFRICOM has called Morocco Africa's premier security exporter.

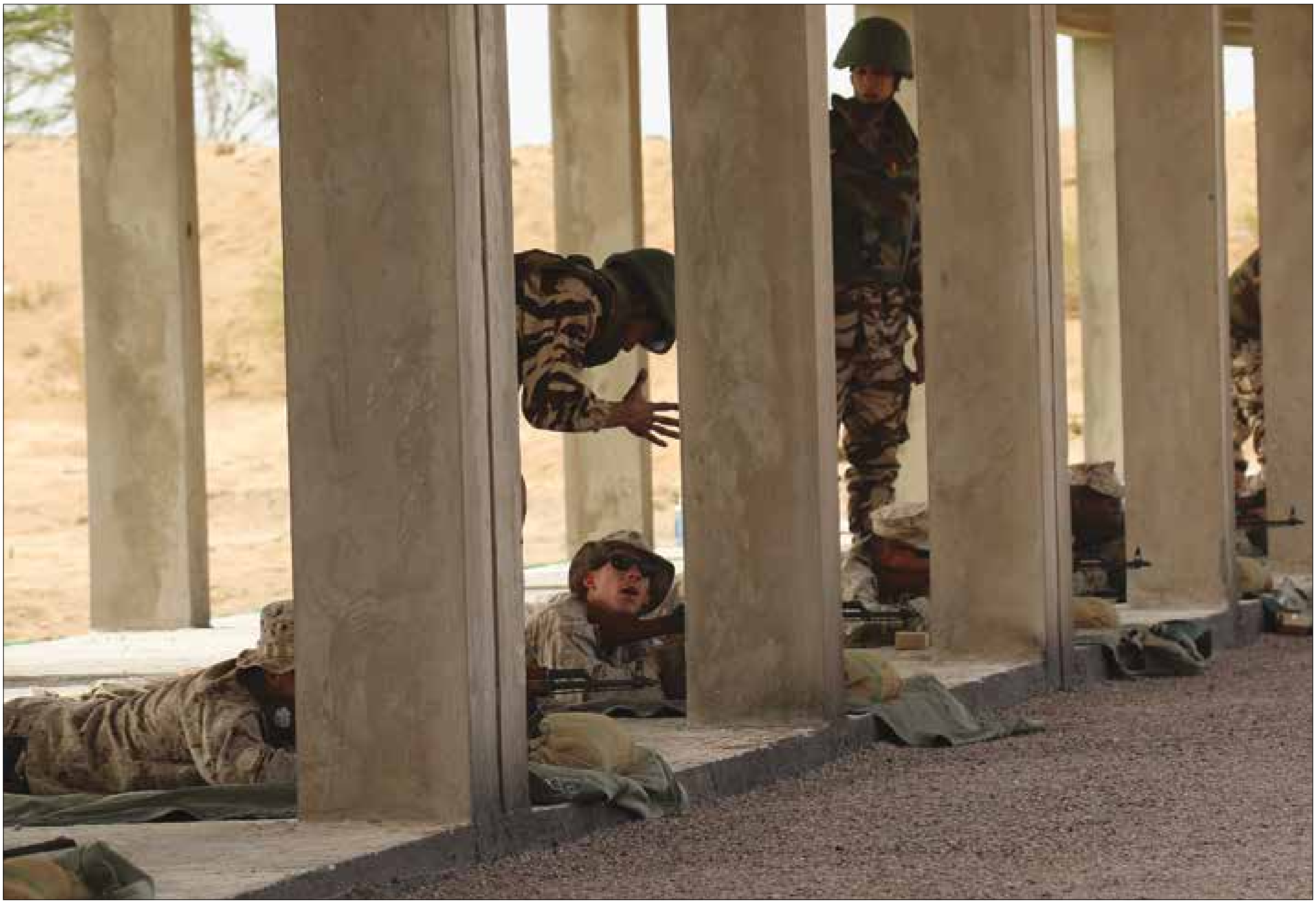
In order to professionalize law enforcement, in 2013 Morocco established the Bureau Central d'Investigation Judiciaire (BCIJ, or Central Bureau of Judicial Investigations) as its elite crime fighting organization. Labeled the "Moroccan FBI" by the media, the BCIJ is the primary law enforcement agency responsible for CT.[13] It operates under the supervision of the public prosecutor of the court of appeals and reports to the General Directorate for Territorial Surveillance, whose agents have the rank of judicial police officers and can conduct investigations, question suspects, and make arrests. They also conduct electronic tracking and eavesdropping upon receipt of written approval from the court of appeals. The Moroccan government has pledged not to use such authorities to deprive citizens of their individual rights.[14] Regarding intelligence collection, the U.S. Federal Bureau of Investigation provides Moroccan government officials training on intelligence analysis, facial recognition, and management.[15]

As a measure of effectiveness, according to BCIJ data, Moroccan security services have interdicted 183 terror cells since 2002, prevented 361 terrorist acts, and arrested more than 3,129 terrorists.[16] The success of Morocco's CT/CVE programs is further indicated by the fact that the country has experienced only two terrorist attacks since 2012—the fewest in North Africa by far.[17] While impressive, human rights organizations have accused Moroccan security services of mass arrests, beatings, and even torture.[18] To avoid creating more terrorists and achieving tactical success at the expense of long-term strategic failure, Moroccans must redouble efforts to purge security services of such abuses.

For judicial reform, the U.S. State Department's Bureau of International Narcotics and Law Enforcement Affairs works with Moroccan partners to increase the professionalism and independence of the judiciary, combat radicalization in prisons, and facilitate reintegration for rehabilitated detainees.[19] Specifically, since 2010, the bureau has worked through Morocco's prison administration, training Moroccan prison wardens to modernize prison management, keep terrorists segregated from the general population, and build more modern and secure facilities.[20]

Counterterrorism is not accomplished through security efforts alone. In addition to security force professionalization, Morocco has implemented an impressive CVE program through policies that ameliorate poverty, improve education, and promote a moderate and peaceful version of Islam. These programs mirror the NSCT's LOE to "counter terrorist radicalization and recruitment."

Addressing poverty is particularly important as recent studies indicate the primary reason Moroccans join terrorist networks is because of economic—not ideological—factors.[21] The average monthly salary for an IS fighter is $1,400, while Moroccans typically earn less than $200 a month (if employed at all).[22] Hence in 2005, King Mohammed VI launched the National Human Development Initiative (NHDI), a



Alpha 3rd Marine Fleet Antiterrorism Security Team from Yorkstown, Virginia, weapons training with Royal Moroccan armed forces during exercise African Lion, April 22, 2019, at Tifnit, Morocco (U.S. Army Reserve/Tynisha L. Daniel)

program that has invested more than $6 billion in its first 10 years of existence and was lauded by United Nations Secretary-General Ban Ki-moon as a model for Africa.[23]

NHDI has served at least 7 million people, with more than 34,000 projects targeting youth and women and providing affordable housing and loans.[24] Despite its popularity, NHDI has been criticized for lacking transparency and encouraging patronage due to centralization of decisionmaking over funds disbursement. As such, some have called for greater transparency and involvement of regional councils in program execution.[25]

Regarding education, a recent study indicates the majority of the 1,600 Moroccans who joined IS and affiliated groups did not have more than a primary school education.[26] Primary and secondary school dropout rates remain high in Morocco (only 18 percent of first graders graduate from high school), and national literacy rates of 55 percent are among the lowest in the region.[27] In addition, low daily attendance rates and teacher absenteeism leave young people vulnerable to radicalization.[28] In response, the U.S. Agency for International Development works with civil society organizations to enhance reading instruction. In addition, the agency facilitated a Millennium Challenge Corporation compact (grant) for $450 million to increase access to higher quality secondary education.[29]

Drawing on his religious legitimacy as Commander of the Faithful, King Mohammed VI has worked to promote moderate and peaceful interpretations of Islam.[30] Specifically, Morocco established satellite television channels that promote the official government version of Islam, including the Sufi and Maliki traditions, to counter Persian Gulf stations that broadcast more extremist Wahhabist principles.[31] Representing a notable innovation, in 2015, Morocco's Ministry of Islamic Affairs created an imam training academy in Rabat that trains not only Morocco's 50,000 imams but also hundreds of imams from elsewhere in Africa, Europe, and Asia in moderate Islam.[32] Additionally, the king created the Mohammedan League of Ulema to promote research in moderate Islam, ensure conformity in Moroccan school curricula, and conduct youth outreach.[33] Morocco also regulates fatwas (religious rulings) by requiring their issuance through a single religious authority—the Higher Scholastic Council.[34] Lastly, Morocco monitors all mosques within the country to deter preaching of radical sermons.[35] While government oversight appears to constrain freedom of religion, clearly some effort to intervene against militant Islam seems justified to address catalysts for radicalization. However, such reforms must necessarily be undertaken by an actor seen to have religious legitimacy and not by an external power such as the United States, which would undoubtedly result in popular backlash.

Examining Morocco in the context of the new NSCT demonstrates the opportunities that exist in supporting and investing in partner nations' CT and CVE efforts. While problems still exist within Morocco, the effectiveness of its programs in limiting attacks and preventing radicalization is evident. The United States should uphold Morocco as an example for other countries in the region and capitalize on Morocco's status as a premier exporter of security. Encouraging and enabling the success of countries like Morocco is a powerful way to diminish the terrorist threat to the world and to convincingly demonstrate that "America First" does not equal America alone. **JFQ**

Notes

[1] Michael R. Pompeo, "Press Statement on President Trump's National Strategy for Counterterrorism," Department of State, October 4, 2018, available at <www.state.gov/president-trumps-national-strategy-for-counterterrorism/>.

[2] *National Strategy for Counterterrorism of the United States of America* (Washington, DC: The White House, October 2018), 1, available at <www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf>.

[3] Jay Figurski, "Information Paper: Morocco Overview," U.S. Africa Command J52, June 4, 2018, 1.

[4] "Morocco," *The World Factbook* (Washington, DC: Central Intelligence Agency, 2019), available at <www.cia.gov/library/publications/the-world-factbook/geos/mo.html>.

[5] "U.S. Relations with Morocco," Bilateral Relations Fact Sheet, Bureau of Near Eastern Affairs, Department of State, July 19, 2018, available at <www.state.gov/r/pa/ei/bgn/5431.htm>.

[6] *Integrated Country Strategy: Morocco* (Washington, DC: Department of State, August 15, 2018), 2, available at <www.state.gov/wp-content/uploads/2019/01/Morocco.pdf>.

[7] *National Strategy for Counterterrorism of the United States of America*, 24.

[8] Figurski, "Information Paper: Morocco Overview," 2.

[9] Ibid.

[10] Meeting with Colonel Andrew Hamann, U.S. Defense Attaché, U.S. Embassy Morocco, Rabat, Morocco, March 13, 2019.

[11] Figurski, "Information Paper: Morocco Overview," 2.

[12] Ibid.

[13] Assia Bensalah Alaoui, "Morocco's Security Strategy: Preventing Terrorism and Countering Extremism," *European View*, July 1, 2017, available at <https://journals.sagepub.com/doi/10.1007/s12290-017-0449-3>.

[14] *Country Reports on Terrorism 2015* (Washington, DC: Department of State, June 2, 2016), 205, available at <https://2009-2017.state.gov/documents/organization/258249.pdf>.

[15] Ibid.

[16] "Tents: 57 Cells Have Been Dismantled and 643 Moroccans Killed in Iraq and Syria," *Lcom2.com* (Rabat), October 1, 2018, available at <http://lakome2.com/societe/42581.html>.

[17] Number of terrorist attacks in North Africa from 2012 to 2018 ranked from least to greatest: Morocco (2), Tunisia (89), Algeria (115), Egypt (1,991), and Libya (2,262). Data for 2012–2017 are derived from the *Global Terrorism Database*, a project of the University of Maryland and the National Consortium for the Study of Terrorism and Responses to Terrorism, available at <www.start.umd.edu/gtd/>. See also "List of Terrorist Incidents in 2018," available at <https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_2018>.

[18] See "Morocco/Western Sahara: Events of 2017," in *World Report 2018* (New York: Human Rights Watch, 2017), available at <www.hrw.org/sites/default/files/world_report_download/201801world_report_web.pdf>; see also "Morocco: Dozens Arrested Over Mass Protests in Rif Report Torture in Custody," Amnesty International Web site, August 11, 2017, available at <www.amnesty.org/en/latest/news/2017/08/morocco-dozens-arrested-over-mass-protests-in-rif-report-torture-in-custody/>.

[19] *Country Reports on Terrorism 2017* (Washington, DC: Department of State, September 19, 2018), 149–150, available at <www.state.gov/reports/country-reports-on-terrorism-2017/>.

[20] Ibid.

[21] Moha Ennaji, "Recruitment of Foreign Male and Female Fighters to Jihad: Morocco's Multifaceted Counter-Terror Strategy," *International Review of Sociology* 26, no. 3 (September 5, 2016), 552, available at <www.tandfonline.com/doi/full/10.1080/03906701.2016.1244954>.

[22] Ibid.

[23] Ahmed Charai, "Morocco's Role in Supporting Human Development in Africa," *Huffington Post*, May 25, 2016, available at <www.huffingtonpost.com/ahmed-charai/moroccos-role-in-supporti_b_7434738.html>.

[24] "Talking Points of Ambassador Nasser Bourita at the Open Briefing of the UN Counter-Terrorism Committee," New York, September 30, 2014, available at <www.un.org/sc/ctc/wp-content/uploads/2015/05/Statement-by-Secretary-General-Nasser-Bourita-MFA-Morocco.pdf>.

[25] Ibid.

[26] Bahija Jamal, "Moroccan Counter-Terrorism Policy: Case of Moroccan Female Migrants to ISIS," *International Annals of Criminology* 56, spec. issue 1–2 (November 2018), 3, available at <www.cambridge.org/core/journals/international-annals-of-criminology/article/moroccan-counterterrorism-policy-case-of-moroccan-female-migrants-to-isis/898D11702AE6B8AA66BD3BA5B068A6C3>.

[27] See "Morocco: Education," U.S. Agency for International Development, May 7, 2019, available at <www.usaid.gov/morocco/education>.

[28] *Integrated Country Strategy: Morocco*, 32.

[29] "U.S. Relations with Morocco."

[30] Ahmed Abaddi, "Morocco's Deradicalization Strategy," Maghreb Roundtable Series, Center for Strategic and International Studies, June 24, 2013, available at <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/130624_Summary_Abaddi.pdf>.

[31] Jack Kalpakian, "Current Moroccan Anti-Terrorism Policy," *Real Instituto Elcano*, May 13, 2011, 5, available at <www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/international+terrorism/ari89-2011>.

[32] *Country Reports on Terrorism 2017*, 149.

[33] Ibid.

[34] Abaddi, "Morocco's Deradicalization Strategy," 2.

[35] Jamal, "Moroccan Counter-Terrorism Policy," 6.

Troops watch activity on Omaha Beach as their LCVP landing craft approaches shore on D-Day, June 6, 1944 (U.S. Army Signal Corps/U.S. National Archives)

Why Normandy Still Matters

Seventy-Five Years On, Operation *Overlord* Inspires, Instructs, and Invites Us to Be Better Joint Warfighters

By Bryon Greenwald

Dr. Bryon Greenwald is a Professor of History in the Joint Advanced Warfighting School at the National Defense University.

The 50-mile stretch of French coastline running from midway up the Cotentin Peninsula east to the Orne River is hallowed ground for all who cherish democracy and the rule of law and the freedom and economic prosperity those values permit. There, on June 6, 1944, Allied forces conducted an enormous amphibious invasion across five beaches—Utah, Omaha, Gold, Juno, and Sword—that caught the Germans by surprise and initiated the end of Nazi reign over Europe. The invasion not only enabled American, British, Canadian, French, and other forces to join the Russians in defeating Germany, but it also allowed them to advance far enough east to prevent Soviet suzerainty over most of Western Europe after the war. In its success, Operation *Overlord* ushered in an open, democratically based economic system that has since expanded beyond its meager beginnings and improved the lives of hundreds of millions of Europeans.

This article celebrates the success and sacrifice of Operation *Overlord* on its 75th anniversary, acknowledges both the achievements and mistakes made in planning and execution, and asks readers to compare the abilities of the current joint force with those of World War II. Geared to those who are familiar with, but not expert in, the critical components of the operation, this article reviews key aspects of the invasion and offers insight into the difficulty of orchestrating such a complicated joint and multinational endeavor at a time when radio communications were in their analog infancy. The article also provides teaching points for emerging military strategists and planners and critiques the operation. Finally, the article asks the reader to question whether today's joint force could achieve something similar, not in size or scale, but sophistication, even with the benefit of global digital command and control suites.

As anniversaries go, the 75th anniversary of Operation *Overlord* holds special significance. As with all the major battles of World War II, it will certainly be one of the last major anniversaries where any of the participants are still living.[1] As such, their sacrifice in that mighty endeavor should not go unnoticed. And although it occurred almost a lifetime ago, the Allied effort to plan and execute the invasion still provides an extraordinary opportunity to examine the difficulty of planning and conducting integrated, all-domain, and joint and combined forced-entry operations against a lethal enemy whose antiaccess/area-denial preparations were immense—something that today's joint force is just now reexamining after spending nearly a generation in counterinsurgency operations. Finally, as Russia and China continue to act aggressively on the world stage, this anniversary may turn out to be one of the last to occur during the relatively peaceful interregnum in Great Power competition the world has enjoyed since the end of the Cold War. Thus, 75 years after airborne troops leapt into the dark French night and thousands of aircraft and hundreds of warships protected dog-faced soldiers as they spilled from plywood landing craft on to fire-swept beaches, the efforts of our forefathers to plan and conduct Operation *Overlord* should inspire us, instruct us, and invite us, as a joint force, to improve our ability to plan and execute all-domain operations.

An Inspiration for All

The invasion of Normandy inspires us by its sheer audacity, its enormous size and scale, and, of course, the personal courage of those involved. To describe the invasion as audacious, however, understates the precarious, one-shot, roll-of-the-dice nature of the event. At the tactical level, the Allies prepared for the attack almost within eyesight of German forces. At their closest points, Britain and the European coast are a mere 20 miles apart. Many of the 120 German radar sets clustered from Calais to Guernsey could easily spot ships and aircraft moving in the English Channel.[2] Portsmouth and Southampton, two of the main ports from which British forces would sail, are only 100 miles from Normandy. In today's strategic environment, that would be the same as launching an invasion from an intermediate staging base like Taiwan toward mainland China or from Kaliningrad to Sweden.

At the operational level, the Germans expected the attack, but could not pinpoint exactly where or when it might occur. Many suspected the Allies would attack across to the Pas-de-Calais, continue through the German industrial base in the Ruhr, and on to Berlin. This avenue offered the most direct route and gave Allied aircraft the greatest amount of loiter time over the invasion area, but it also meant capturing a heavily defended port and fighting through the majority of German forces, including Panzer divisions, in the west. Some senior German leaders, however, suspected that the attack might come elsewhere. The failed Anglo-Canadian attempt to attack the heavily defended port at Dieppe in August 1942 proved just how difficult that approach would be in the future and hinted at an over-the-beach invasion.

Generalfeldmarschall Erwin Rommel, in charge of all western defenses from the Bay of Biscay to Denmark, initially leaned toward Calais, but considered a Normandy invasion likely. He focused his attention on what the Allies would call Omaha Beach because its long concave waterfront resembled Salerno, which the Allies had assaulted in September 1943. Even Adolf Hitler had a premonition of an attack in Normandy, but hedged his bet by predicting the Allies would invade in both places.[3] Fortunately, in doing so he unwittingly supported the Allied deception plan designed to make the attack on Calais appear as the operational main effort.

Finally, the assault was strategically audacious. Other amphibious assaults during the war were no less daring, difficult, or deadly, but they were essentially "away games" for both sides, fought by the Allies against second-tier or lesser forces that were unprepared, undersupplied, isolated, or retreating. With Operation *Torch* in North Africa, the Allies conducted an error-filled assault on Vichy French forces in a secondary theater and later defeated Rommel's beleaguered army in Tunisia.[4] In Operation *Husky*, the successful yet flawed amphibious landing on Sicily, the Allies learned the difficulty of transitioning from ship to shore and air to ground against a wounded but deadly enemy.[5] Even in the Pacific, as ferocious as the fighting from Tarawa to Okinawa was, the Americans isolated the Japanese, cut their air and naval support, and pounded them relentlessly with naval gunfire, artillery, and aviation.[6] Victory in those battles was bloody, but never in doubt. Moreover, while all those amphibious assaults carried tactical and operational risks, their outcome was not in question, and beyond North Africa, even their failure could not derail Allied strategy.

The invasion of Normandy, however, was fought on German ground, although their lease on French territory was only 4 years old. And while Hitler's boasts of *Festung Europa* (Fortress Europe) and the impenetrable Atlantic Wall were largely just that, once he placed Rommel in charge in early 1944, the defenses improved dramatically. With characteristic energy, Rommel revitalized languid units and layered the coast with hundreds of pillboxes and tank traps, thousands of obstacles, and millions of mines, many deviously placed to be underwater at high tide.[7] And unlike in other amphibious assaults, the Germans could reinforce the assault area with Panzer and other units from as near as the Pas-de-Calais and as far away as the Eastern Front.

Beyond all of these tactical and operational factors, Normandy posed the likelihood of strategic and political failure. If Rommel had succeeded in throwing the Allies back into the Channel, the chance of a follow-on Allied attack within a year or two was extremely remote. While General George Patton's Third Army was sitting in England in reserve, it would take time to reconstitute losses in landing craft. Besides, not only was Prime Minister Winston Churchill already antsy and given to visions of a repeat of Gallipoli, the Somme, and Passchendaele, with Allied blood filling the Channel, but the British were also running out of men and had started cannibalizing divisions for infantry replacements even before the invasion started.[8] There was simply no more ink in the British well to spill on a second attempt. Operation *Overlord* was their only opportunity.

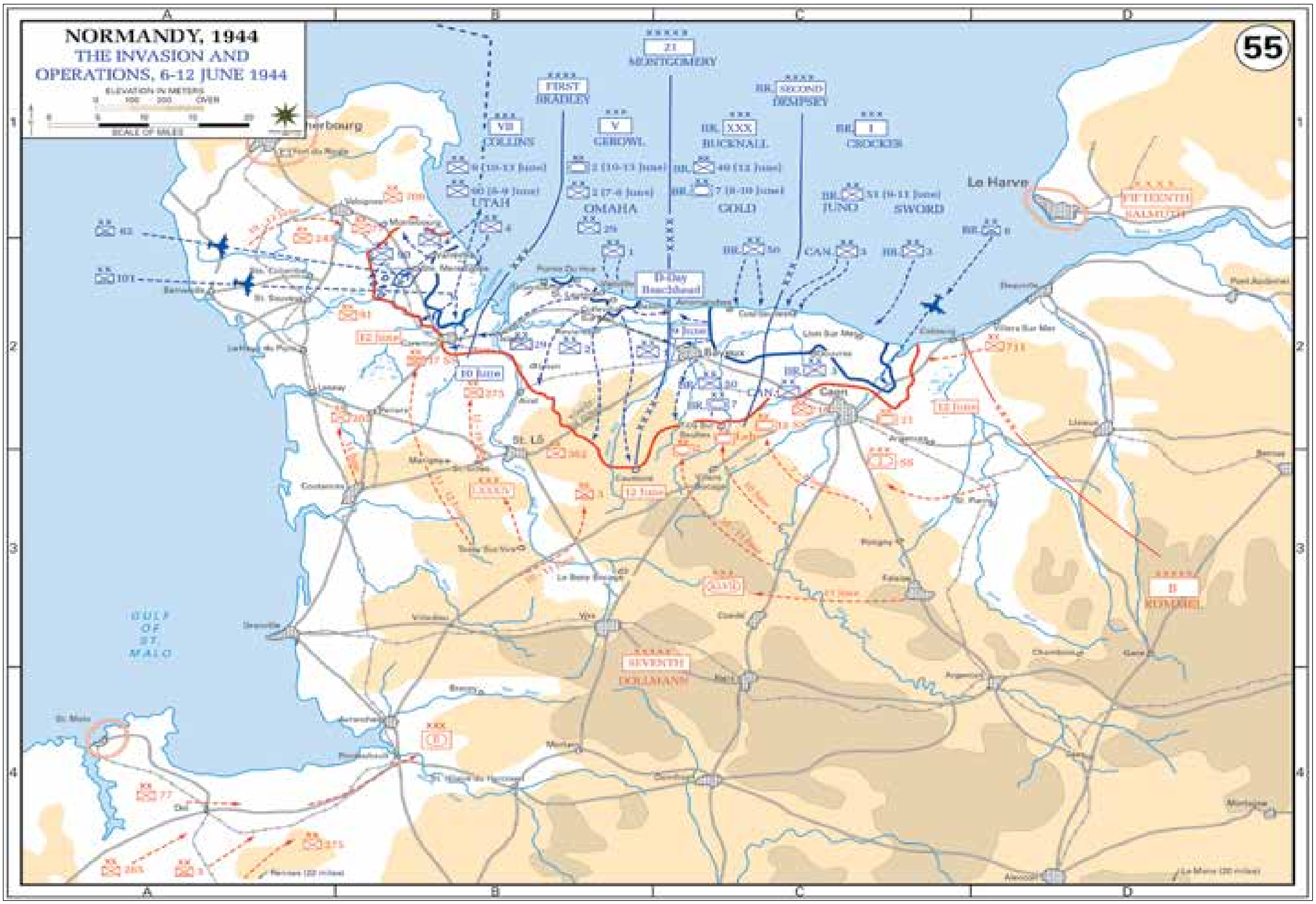
Exacerbating an initial defeat in France, any Allied pause to regroup would have allowed Hitler to expand his V-weapons campaign, which was already ravaging London. The combination of the two might have caused Churchill's government to fall and resulted in a negotiated peace. Finally, an Allied defeat in Normandy would have freed the majority of German units to turn back to the east, where they might battle Russia to a stalemate and possibly a negotiated peace as well. *Overlord* really was a one-shot effort.

Despite a shortage of British manpower and barely enough transport to conduct the invasion, the size and scale of the operation was breathtaking. Today's strategists and operational planners can only begin to fathom the magnitude of the combined force and complexity involved in marshalling, moving, and synchronizing its effects in a world where analog communication was difficult and digital technology nonexistent. Crammed into England at over 2,000 camps and airfields were over 1.5 million American and 600,000 British servicemen organized into 20 U.S. and 16 British, Canadian, and Polish divisions as well as scores of other ground, sea, and air forces. Another 37 U.S. divisions were to follow, either through England or directly from America.[9] The initial invasion launched five divisions destined for four nearly contiguous beaches running east to west—Sword, Juno, Gold, and Omaha—and one outlier on the Contentin Peninsula closer to the port of Cherbourg near Utah Beach. Three other divisions followed in trail.

Transporting these forces across the Channel from 171 British ports at night under radio silence were nearly 7,000 vessels operated by almost 200,000 sailors, coastguardsmen, and merchantmen in Operation *Neptune*, a supporting operation to *Overlord* that focused on the crossing and beach landings. This armada included 138 destroyers, cruisers, and battleships. These warships provided this fleet's seapower, but the landpower needed to retake Europe arrived on 46 different types of landing craft, approximately 4,200 in all, including the critically short landing ship tank or "long slow target" capable of carrying half an armor battalion and depositing it on the beach via its massive bow doors.[10] This enormous and diverse force rendezvoused about 13 miles south of the Isle of Wight, in Area Z, or as it was called "Piccadilly Circus," and led by 300-odd minesweepers, chopped across the Channel in 5 and then 10 lanes averaging about 800 yards wide in search of the midget submarines that marked the boundaries of the invasion area. Ahead of these forces, two U.S. and one British airborne division, 23,400 troops in all, dropped at night to secure key points behind Utah Beach and seal the eastern flank along the Orne River from counterattack. Moving these men were almost 1,400 transports and over 760 gliders (416 with U.S. forces and at least 250 with British). Blasting the far shore and sweeping the skies over this force were nearly 4,500 bombers and 4,000 fighters. By sunset at 10:06 p.m. local time, the Allies had placed over 155,000 men, 1,550 tanks, and 12,500 vehicles ashore.[11]

Beyond its size and scope, what one soldier in the German 716th Static Infantry Division described as a "gigantic city at sea," the force contained several specialty vehicles that spoke to the value of innovation and organized industrial strength.[12] Operating with the invasion force were Duplex Drive tanks that could swim ashore albeit under the right conditions; Crocodiles, tanks turned into tracked flamethrowers; Crabs, flail tanks fitted with heavy chains on a rotating cylinder that cleared minefields; Bobbins, tanks that rolled out a reinforced canvas road to drive on as they moved forward; Armored Ramp Carriers (ARKs), tanks that carried deployable ramps instead of turrets; and Ducks (DUKWs), 6-wheeled amphibious vehicles for moving men, 105-mm howitzers, and supplies ashore.[13] Finally, chugging along just behind the force were a flotilla of tugs hauling three miracles of modern industry—two artificial floating harbors and a pipeline under the ocean (PLUTO).

Given the difficulty expected in seizing a heavily defended deep-water port intact, the Allies, largely through British initiative, decided to bring two enormous ports with them. While logisticians intended to protect all five invasion beaches with "gooseberries" or artificial breakwaters, two beaches—Omaha and Gold—would serve as sites for the Allies two artificial floating harbors, codenamed Mulberries. Consisting of several unique elements, including floating steel pier heads and roadways and massive hollow concrete breakwaters

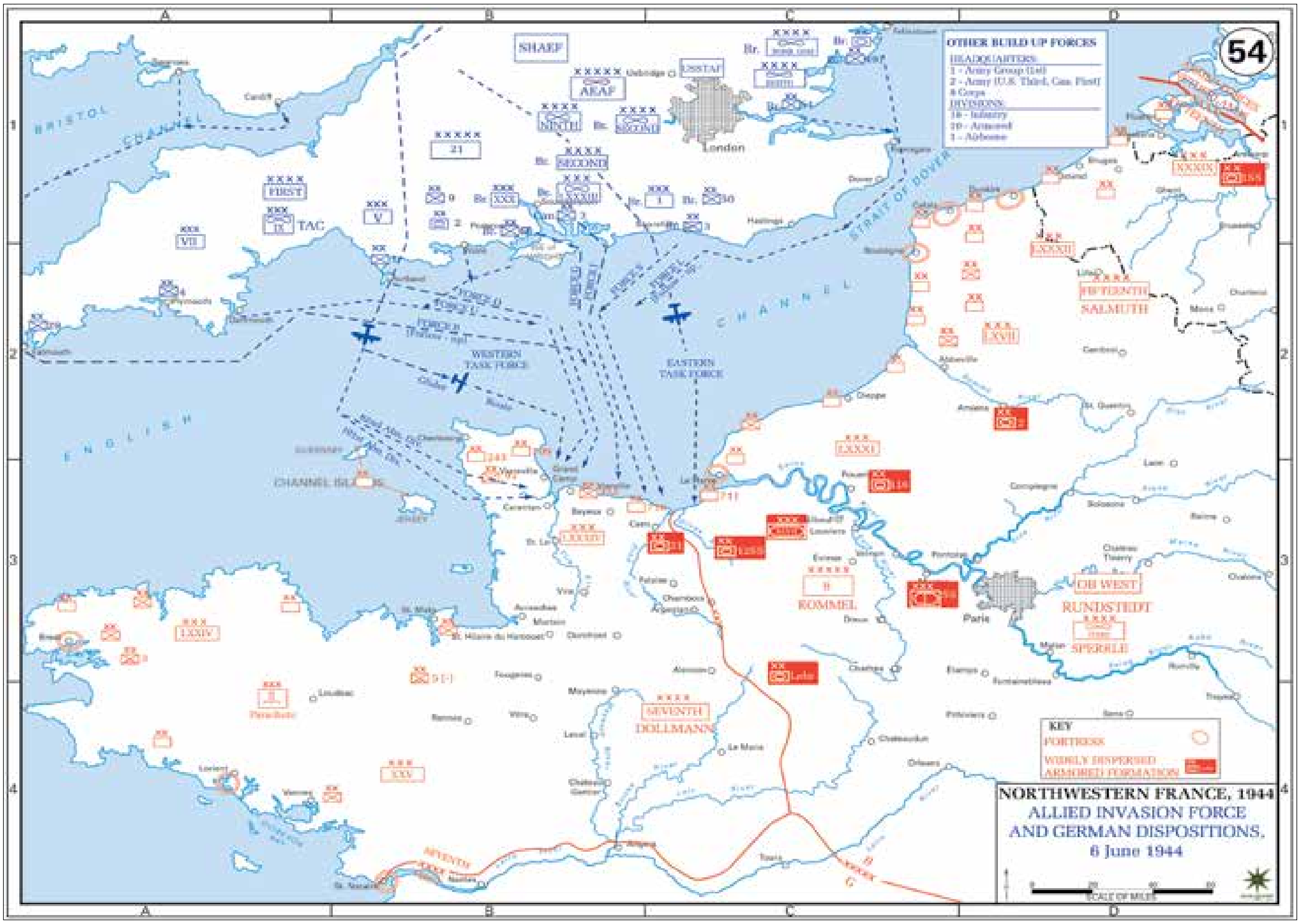


Following three Allied airborne divisional drops, five U.S., British, and Canadian divisions assaulted the Normandy beaches (Courtesy West Point Department of History)

for the inner harbor, these structures consumed about 661,000 U.S. tons of concrete and 100,000 U.S. tons of steel and took 45,000 men 8 months to construct. Although a tremendous storm (June 19–22) destroyed the American Mulberry at Omaha, the British port at Gold Beach survived and proved useful throughout the Normandy campaign.[14] Lastly, if 19th-century armies marched on their stomachs, modern armies motored forward on petroleum. To keep their highly motorized and mechanized armies moving, the Allies developed and laid hundreds of miles of steel PLUTO. Unfortunately, while engineering marvels, these pipelines suffered from accidents with ships' anchors and breakage that limited their timely transport of fuel. This shortfall led to an early adaptation of existing transport capacity, the Red Ball Express, as supply officers commandeered 7,000 2.5-ton trucks to transport 4,000 tons of fuel, mostly in 5-gallon jerricans, on one-way highways to supply points in the First and Third U.S. Army areas.[15]

Notwithstanding the countless acts of bravery noted over the last generation of conflict in Afghanistan and Iraq, the personal courage demonstrated during Operation *Overlord* by men at all levels still inspires and serves as an example to us all. From Supreme Allied Commander General Dwight D. Eisenhower through component commanders and senior leaders, to the engineers, Seabees, medics, and infantrymen that first landed in Normandy, their actions and level of personal responsibility represent our better selves even in the darkest of times.

Consider Eisenhower's example of humble strategic leadership. At 4:30 a.m. on June 4, he postponed the invasion for 24 hours due to extremely bad weather, knowing that there were only 4 days—the 5th, 6th, 19th, and 20th—in June that provided the right combination of a late rising moon and early morning rising tide to create the opportunity for a successful assault. Seventeen hours later, as wind and rain lashed the windows of his temporary headquarters at Southwick House near Portsmouth, Eisenhower received a forecast update indicating a mild break in the weather for June 5 and 6. After polling his commanders, he calmly assessed the situation, wondering aloud, "How long can you hang this operation on the end of a limb?" He committed to launch the assault with a final go/no-go weather update at 4:15 a.m. on June 5. At that meeting, after receiving confirmation that the weather break would hold, he announced without any pomp, "Okay, we'll go." He then returned to his private trailer where he handwrote a note taking complete and personal responsibility for the invasion if it failed and stuffed it in his wallet. Finally, he visited Greenham



While fixing German attention on Dover, England, Allied forces consolidated and sailed toward Normandy. Hours earlier, paratroopers and glider forces took off to seize key objectives on the Orne River and Cotentin Peninsula (Courtesy West Point Department of History)

Common airfield to meet paratroopers from the 101st Airborne Division, staying to watch the last of their aircraft take off, saluting with tears in his eyes and knowing that by dawn many of those he met would be dead.[16]

Then there was the calmness and clarity of men under fire, men like Rear Admiral John Leslie "Jimmy" Hall, Jr. Known in modern joint parlance as the Commander, Amphibious Task Force, Hall directed the assault on Omaha Beach from the USS *Ancon*. In the midst of the assault, he cautioned a very anxious Major General Clarence Huebner, Commander of the 1st Infantry Division, to be patient and let the stalemated situation on Omaha develop further, thereby preventing Huebner or First Army Commander General Omar Bradley from issuing what would have been a disastrous order to evacuate the beach.[17] Another example is Brigadier General Theodore Roosevelt, Jr., the Assistant Commander of the 4th Infantry Division, who landed 2,000 yards off course with the first wave at Utah Beach and calmly decided that "we'll start the war from here."[18] Brigadier General Norman "Dutch" Cota, Assistant Division Commander of the 29th Infantry Division, on landing in the second wave at Omaha Beach, found the men leaderless and not moving. Walking westward under fire, he admonished troops to "get off the beaches," encouraged the "Rangers to lead the way," and then, after machine gun fire had stalled an attack, personally led a charge through a gap in the wire and up the bluff east of Vierville-sur-Mer that enabled men from the 116th Regimental Combat Team (RCT) to outflank German defensive positions at the D-1 (Vierville) draw. Regimental commanders like Colonels Charles Canham (116th RCT) and George Taylor (16th RCT) similarly led from the front and exhorted men to advance.[19]

The Rangers scaled the 100-foot cliffs of Pointe du Hoc while dodging German grenades and rifle fire, and lieutenants, sergeants, and privates led platoons, squads, and confused groups of men forward—always forward. Finally, any of the thousands of frightened men who, scrambling to exit their Higgins boats, "tumbled out just like corn cobs off a conveyor belt" and were hit by fire from German machine gun nests covering "Bloody Omaha."[20] One only has to read the names on the 29th Infantry Division and Engineer Special Brigade monuments or walk up the slopes behind Omaha Beach about 500 yards to a great granite obelisk engraved with the names of the 627 men from the 1st Infantry

Division who died that day, including 3 names etched in gold signifying that they won the Medal of Honor, to realize that uncommon valor was a common occurrence on June 6, 1944.

Instruction for Today

Despite the passage of time, Operation *Overlord* continues to offer valuable lessons across a range of critical topics. Chief among these lessons is the importance of getting the overarching war policy correct through coherent and clear-eyed national security policy planning. To paraphrase Carl von Clausewitz, senior leaders should avoid turning the purpose of war into something alien to its nature—a mistake many contend the United States made in Iraq. Other lessons include the need to align strategic goals with higher policy ends, the criticality of determining and sequencing of essential tasks, and the value of developing an operational approach to achieve strategic and operational objectives and then planning in reverse from the point of success to ensure forces and actions are arranged, sequenced, and supported appropriately in time and space.

Lessons on Policy Planning and Strategic Alignment. Against the backdrop of the Vietnam War and the wars in Afghanistan and Iraq, Operation *Overlord* stands as an example of what coherent policy, grand and theater strategy, all-domain operational design, and organizational acumen can achieve. At the level of Allied policy, in late summer 1940, with Germany having conquered most of Western Europe and now bombing and preparing to invade Great Britain, U.S. Army and Navy leadership shrugged off decades of planning for a potential war with Japan and came to the conclusion that the survival of Great Britain and its Empire was in the best interest of the United States. As the now historic memorandum sent by Chief of Naval Operations Admiral Harold Stark to President Franklin D. Roosevelt in November 1940 stated, "If Britain wins decisively against Germany, we could win everywhere; but . . . if she loses the problem confronting us would be very great; and while we might not *lose everywhere*, we might, possibly, not *win anywhere*."[21] Thus, despite planning for a war with Japan since 1907, the national security apparatus recognized the greater threat and adjusted its overarching policy accordingly. That the Nation would remain committed to this policy after the Japanese attack on Pearl Harbor speaks to the quality of analysis and the strength of its conclusion.

This tectonic shift in policy quickly led the United States and Britain to expand senior military staff talks on global strategy and resulted in a series of Allied decisions over the next few years that framed the overall strategic direction for the rest of the war. As they applied to Normandy, these decisions were to avoid negotiated settlements and seek the complete defeat of the Axis nations; defeat "Germany First"; invade North Africa in 1942 instead of attempting a cross-channel attack; resource the Combined Bomber Offensive to attack German forces, resources, and cities; and invade Northwest Europe in 1944.[22] All these decisions demonstrate to contemporary officials, as Clausewitz notes, the importance of understanding the political purpose of war and the need to work hard to get the policy and strategy aligned as correctly as possible. For as the Germans learned, no amount of operational or tactical virtuosity can rescue a military force from bankrupt strategic direction.[23]

Lessons on Determining and Sequencing Essential Tasks. Before tackling any of its strategic objectives, however, the United States had to complete a series of essential tasks. It needed to raise, organize, train, and equip the military forces of all four Services (Army, Army Air Forces, Marines, and Navy) to a level where they could fight and sustain a series of global campaigns for years.[24] Before contemplating an attack on Europe, the Americans needed to sustain the British, who were rebuilding their own military after Dunkirk and suffering a 60 percent decrease in foodstuffs and fuel due to the success of the German U-boat campaign against commercial shipping in the Atlantic.[25] Thus, American and British forces needed to win the Battle of the Atlantic before they could ever reasonably consider beginning the necessary logistical buildup to support an invasion of the continent. Finally, the Allies had to win control of the air to allow any invasion force a modicum of freedom of maneuver.

In 1942, Army Chief of Staff General George C. Marshall and his Chief of War Plans, Brigadier General Dwight D. Eisenhower, pressed for a direct attack on the Germans as soon as possible, and certainly not later than 1943. Thus, prior to the decision to invade Normandy, the most instructive decision from both a geopolitical and strategic perspective was Roosevelt's July 1942 decision to invade North Africa, which he made against the wishes of his military advisers. Hailed by some today as an example of the value and need for civilian control of the military, the decision makes complete sense in hindsight. Roosevelt wanted American troops in combat against the Germans in 1942, but neither the British nor the American militaries were ready to conduct a contested amphibious landing against the Germans on the coast of France.[26] The British, who had already lost several battles to the Germans and who at that point would have to provide the majority of forces, were accordingly reluctant. And as the clumsiness of American operations in North Africa indicated, U.S. troops and their leaders were simply not ready to take on German forces in an amphibious assault.[27] Even Marshall later intimated that the idea of landing 25 divisions in Europe in 1942 might have been "suicidal."[28] Moreover, as much as General Eisenhower lamented about "wasting resources all over the world," the fact remained that shipping and amphibious craft, two important resources for globally integrated operations, were in short supply—so much so that in 1944, Eisenhower, as Supreme Allied Commander, requested a 1-month delay in launching Operation *Overlord* in order to obtain more "long slow targets."[29]

Eventually, the Americans and British overcame their collective difficulties in North Africa and began to prepare for an invasion of Europe. In February

1943, they formed an integrated planning headquarters under the Chief of Staff to the Supreme Allied Commander (COSSAC), British Army Lieutenant General Frederick Morgan, and selected Normandy as the site of the invasion. In May 1943, as American and British soldiers defeated the Germans near Tunis and captured 275,000 soldiers, their leaders met in Washington, DC, at the Trident Conference and set the date for Operation *Overlord* as May 1944. In the meantime, they would attack through Sicily and on to Italy with the goal of knocking Italy out of the war and forcing the Germans to send reinforcements to stop the Allies. This decision meant the Allies, in a supporting effort to the overall campaign in Europe, would fight a determined German enemy up the mountainous Italian boot on something of a shoestring as the British and Americans withdrew units and diverted supplies to begin the buildup for the invasion of France.[30]

Lessons on Operational Design and Arranging and Sequencing Forces in Space and Time. Although not without issues, the quality of the operational design and joint/combined planning for Operation *Overlord* offers today's leaders and planners an excellent example of integrated all-domain operations.[31] As for operational art and design, Allied planners developed an operational approach that envisioned the arrangement of real and fake forces in England such that the Germans viewed the area near Calais as the main objective and reinforced it accordingly with the bulk of their Panzer units. If successful, this action would give the Allies a better chance to get ashore as a coherent fighting force; to defeat a smaller, less powerful German reaction force; and to win the race to build up more combat power than the Germans could bring to bear in the assault area. Then beginning with the strategic guidance to "enter the continent of Europe and . . . undertake operations aimed at the heart of Germany and the destruction of her Armed Forces," the COSSAC staff developed a concept of operations that integrated the multifaceted deception story with a three-division assault between the Orne and Vire rivers. In late 1943 and early 1944, Eisenhower and his ground commander, British General Bernard L. Montgomery, assessed the plan and found the force too weak. They drove further refinement and expanded it from three to five divisions, increased the airborne forces from less than one division to three, and added Utah Beach as an objective in order to facilitate capturing the vital port of Cherbourg.[32]

Appropriately, the staff identified the key component of the German defense in the west as the Panzer divisions and corps. Known in today's doctrine as the operational center of gravity, the Panzers were the only force with enough mobility and power to threaten the Allied landings; they were the glue that held the German defense together. The foot-mobile infantry had neither the speed nor the punch to stop the Allies, and the Luftwaffe could not provide significant air support because it was defending the skies over Germany from the Combined Bomber Offensive. To protect the landing sites from armored counterattack, the planners used a combination of information, intelligence, joint fires, and maneuver to fix Panzer units near Calais and impede the movement of other Panzer units into the assault area.[33]

First, they reinforced the Fortitude South deception plan by deploying live units to mix with fake ones in eastern England and Scotland and broadcast scripted radio traffic to support the cover plan and augment the action of those units.[34] Second, planners assigned electronic warfare assets, ships, and bombers to execute tactical deception plans (Operations *Taxable* and *Glimmer*) on the night of June 5–6 to trick German radar operators, shore lookouts, and intelligence personnel into believing the Allies were attacking north and east of Le Havre.[35] Third, using Ultra decrypts, overhead imagery, agent reports, and radio intercepts they identified the general locations of several Panzer units and targeted them for bombing, both before and after the assault.[36]

Fourth, as part of the Transportation Plan, the Allies used bombers as part of their operational fires to drop the bridges over the Seine and the Loire rivers, essentially carving out a section of France and isolating it from German units to the east and south of the rivers. Fifth, they used air interdiction to destroy railheads and marshalling yards across France to force Panzer units on to roads, where they would consume precious fuel and could be hit by air or subject to sabotage by the French Resistance. In all these air attacks, the British and American air forces were careful to spread out their attacks, striking twice as many targets outside the Seine/Loire area as in it, to mask their intent to land in Normandy. Sixth, to create a tactical deception and assist inbound airborne forces, planners in Operation *Titanic* dropped special operations forces with amplifiers and recorded combat noise, thousands of rifle and machine gun simulators, and 200 dummy half-sized paratrooper "dolls" or, as the Germans called them, *Explosivpuppen*, in key areas throughout Normandy to confuse the Germans and draw off anti-paratrooper reaction forces.[37]

Finally, planners dropped the 6th British Airborne Division to the east of the Orne River and Caen Canal to blow up bridges over the Dives River, destroy an artillery battery capable of hitting Sword Beach, and capture the bridges at Bénouville and Ranville, which they did with an amazing glider assault.[38] On the west end of the assault area, the 82nd Airborne Division secured the key road junction at Sainte-Mére-Ѐglise and two bridges over the Merderet River, while the 101st Airborne Division captured critical elevated causeways and provided the 4th Infantry Division with a way across the flooded lowlands and off of Utah Beach.

In the end, the combined effect of these actions did indeed delay and impede the movement of Panzer and other units. Even after the Normandy landing, Ultra decrypts confirmed that Hitler remained convinced the main attack was still to come in the area of Calais and would not release the Panzer units there until early August. Closer in, the destruction of the bridges over the Dives River and the defense at the bridge at Ranville forced the 21st Panzer

Panoramic view of Omaha beachhead after it was secured, mid-June 1944 (U.S. Coast Guard/U.S. National Archives)

Division to endure countless air attacks while driving around Caen to attack British and Canadian units from the south instead of more directly from the east. Operation *Titanic* succeeded in dispersing elements of the first-rate 352nd Infantry Division and delayed Task Force Meyer (915th Infantry Regiment) from counterattacking forces struggling ashore at Omaha Beach.[39] Finally, the interdiction of bridges and railheads forced the 2nd SS Panzer Division, Das Reich, located near Montaubon in Brittany, to travel north toward Normandy intermittently by rail and road. At great risk, the French Resistance blew up fuel dumps, sabotaged rolling rail stock, destroyed rail lines, and organized small ambushes. All told, the Das Reich division took 17 days to move the 350 miles from Montaubon to Normandy, a journey that should have taken just 3 days.[40]

Not Everything Will Go According to Plan, Failures to Anticipate and Prepare Will Occur, and Mistakes Will Happen. Despite its ability to deceive, delay, and disrupt the Germans, the Allied assault was not a complete success. As darkness fell on Normandy, the Allies had achieved none of their D-Day objectives other than getting ashore. At Utah, the 4th Infantry Division had yet to link up with the 82nd or 101st airborne divisions. At Omaha, the beachhead was barely a mile deep and the beach itself was a disaster. At Gold, the 50th British Division after a tough fight had failed to take either Port-en-Bessin-Huppain or Bayeux or link up with the Americans at Omaha. At Juno, the 3rd Canadian Division advanced farther than any other unit, but failed to secure the high ground near the Carpiquet airfield west of Caen. And finally, at Sword Beach, the British 3rd Division failed to take Caen.

At the tactical level, the tail end of the storm that initially delayed the invasion and caused the Germans to believe that nothing would happen on June 6 made bombing by sight difficult and sailing in small craft treacherous. But beyond the weather, errors in judgment cost lives and wasted tactical efforts, particularly on hard-fought Omaha Beach. B-24

Equipment and armored vehicles, some damaged, stretch across sands in Normandy where Allies seized beachhead, June 6, 1944 (Courtesy AP Photo)

Liberator pilots forced to bomb using radar and flying perpendicular to Omaha feared hitting the approaching landing craft. As a result, the lead pilots held their fire for an additional 5 to 20 seconds and 450 bombers ended up dropping their 13,000 bombs harmlessly on crops and livestock miles behind the German defenders. At sea, 6,000 meters (more than 3 miles) off Omaha, Army lieutenants and Navy and Coast Guard ensigns discussed the sea state with its 4-foot chop. Some considered it too dangerous to launch their Duplex Drive swimming tanks and artillery-carrying DUKWs that far out. Others debated and made the fateful decision to launch anyway. In one case, 27 of 32 Duplex Drive tanks and most of the artillery foundered and sunk. A number of Soldiers drowned and the Americans lost a great deal of the firepower they needed to suppress the 35 German pillboxes, 8 huge bunkers, and 85 machine gun nests guarding Omaha Beach.[41]

Exacerbating these tactical errors were organizational decisions made by First U.S. Army Commander General Bradley that limited the amount of naval gunfire support or specialized armored vehicles available to the troops on Omaha. In the spring, Army Chief Marshall sent Bradley one of the Army's experts in amphibious warfare, Major General Charles Corlett, from the Pacific. Despite a wealth of advice, Bradley and Eisenhower displayed no interest in learning from Corlett, viewing efforts in the Pacific as "bush league." Corlett warned Bradley that he did not have enough naval gunfire to support the landings properly or enough ammunition for the upcoming land battles, both of which were ultimately proven correct. Moreover, despite Montgomery's encouragement, Bradley dismissed the value of flail and other types of tanks offered by the British—only to wish later that he had them at Omaha.[42]

At the operational level, intelligence failures influenced events on D-Day and beyond. First, Allied intelligence completely missed or "lost" the location of the 352nd Infantry Division, a first-rate unit initially thought to be near St. Lô, but which the Germans moved forward in May. On D-Day, it stretched from the Vire River to Arromanches, with at least two infantry battalions and a light artillery battalion bolstering the defense of elements of the second-rate static 716th Infantry Division at Omaha Beach. Second, the Americans utterly misunderstood the nature of the *bocage* country that filled the Normandy region south of the immediate beach area. With thick, impenetrable Norman hedgerows and sunken ox-cart tracks bordering thousands of small farm fields, the area was superb defensive terrain that armor could not breach, traditional artillery could not hit, and infantrymen could not enter without coming under withering machine gun and mortar fire.[43] The terrain provided such a series of natural obstacles that a two- or three-man team could defeat a platoon, a platoon might defeat a company, and a company could slay a battalion. The Allies had over 1 million photographs of the Normandy area and hundreds of intelligence reports, including one from April 1944 by Bradley's First Army that warned that fighting there "be given considerable study." As Bradley later stated, "I couldn't imagine the bocage until I saw it." It was "the damnedest country I've ever seen."[44] One battalion commander was more succinct, noting later that "we were rehearsed endlessly to attack the beaches, but not one day was given to the terrain behind the beaches."[45] This failure to recognize and react to the potential difficulties posed by the bocage country cost the U.S. Army dearly as divisions were bled white fighting south to the St. Lô-Périers Road, the jumping off point for the "breakout" on July 25.

On D-Day, U.S. forces suffered approximately 12,000 casualties, including 8,230 Americans. From D-Day until July 31, Bradley's First Army took 100,000 casualties, including 9,939 in the 29th Infantry Division and 7,876 in the 4th Infantry Division, both of which fought through the bocage. Eighty-five percent of the casualties were infantrymen.[46]

Finally, perhaps the greatest failure in planning and leadership was Montgomery's inability to take Caen, his D-Day objective for the 3rd British Infantry Division at Sword Beach. Montgomery and his army, corps, and division commanders failed to plan backward from their objective. They did not factor in likely confusion on the beach, consider the likely exhaustion and culmination of their initial and follow-on forces, anticipate German counterattacks by elements of the 21st Panzer Division, and provide for additional forces to pass through and take Caen. While the Germans certainly had a role to play with their staunch defense at the Hillman strongpoint and along Périers Ridge, it is clear that the 3rd British Infantry Division faced too many tasks and suffered too many diversions that frittered away its combat power.[47] In essence, Montgomery, Lieutenant General Miles Dempsey, Lieutenant General John Crocker, and Major General T.G. Rennie ignored the timing and tempo of operations, did not mitigate known risks, and failed to arrange their forces such that they would have the staying power necessary to seize their admittedly ambitious objective in the face of likely opposition.[48] Despite relentless Allied air and *résistant* attacks, the Germans managed to reinforce the area with Panzer forces. In some of the largest tank battles of the war, Montgomery and Dempsey would spend the next 45 days attempting to envelop Caen and capture the key operational terrain on Hill 112 that opened the path to Paris and beyond.[49] Meanwhile, the Americans, due to their own failures to anticipate and prepare for fighting in the bocage, would slog forward, grinding through divisions and wearing down Germans forces until their own breakout in Operation *Cobra* on July 25.

The study of Operation *Overlord* teaches today's commanders and planners that designing an all-domain operational approach that keeps the enemy off balance and synchronizes the integrated joint and combined actions of thousands of aircraft and ships and hundreds of thousands of men under the watchful eyes of the enemy is excruciatingly hard to do, let alone do well. It requires an uncommon level of operational understanding and joint knowledge. *Overlord* also warns us to expect that our adversaries may be both lucky and good, and as well-equipped and trained as we are. It cautions those conditioned by decades of all-domain dominance against less than first-tier opponents to expect that even the best plans will go awry and, unlike the Americans in the bocage, we should plan and train for that eventuality as well.

In the end, success in Operation *Overlord* was "a close run thing."[50] It succeeded in part because of America's overwhelming ability to build and deploy a vast array of ships, landing craft, aircraft, tanks, and artillery; in part because of the individual and collective courage of the Allied servicemembers who fought it on the ground, on the sea, and in the air; and in part because the operational design and combined planning for the invasion synchronized all aspects of Allied capability sufficiently enough to provide the slimmest of margins when it mattered most.

An Invitation to Improve

More than answers, Operation *Overlord* invites us to ask questions of ourselves and our ability to operate jointly. Specifically, could we do it again? Not in size, but in effect? Could the United States or NATO repeat an operation as complex as *Overlord*? Are our generals and admirals, colonels and captains, and perhaps most important, the iron majors and commanders who sweat out the critical details, educated and savvy enough to conceptualize, organize, and synchronize an integrated joint/combined operation of *Overlord*-like complexity against a peer competitor?

Beyond our ability to conceive, plan, and synchronize such a complex event, the legacy of Operation *Overlord* invites us to consider if we are ready in unit manpower, equipment, and training readiness to execute combined operations of similar sophistication against Russia, China, or Iran as described in recent discussions of globally integrated operations. Is the Navy seaworthy? Can the Air Force get more than 60 percent of its aircraft airborne at any one time? Are the Army and Marine Corps robust enough to field full-up brigades and divisions without cutting late deploying units to the bone? Are we practiced enough in our Service-based skills that we can even attempt to integrate jointly?

For the joint force, this calls into question whether we can integrate seamlessly above Service level, on the fly, at night, under radio silence, without GPS, just as the forces did in approaching Normandy. Are we resilient enough to take a punch on the chin (like our forefathers did at Bataan, Kasserine Pass, or Anzio) and recover? Or are we too fragile—too unprepared intellectually, too thin in necessary force structure, or too technologically dependent—to win the battles, campaigns, and wars we portend with Great Power competition?

Finally, do we have the requisite mental and command flexibility, organizational diversity, and depth to recover from an adversary's first bloody surprise moves and fight back to tactical, operational, and strategic positions of dominance? Do we have, as the Capstone Concept for Joint Operations 2030 asks, the "strength, agility, endurance, resilience, flexibility, and awareness" to recover and adapt? Today, are we in a joint "Boxer's stance" ready to react, punch, and counterpunch, just as the men in Normandy did 75 years ago? Will we be a "globally integrated, partnered joint force that is designed and able to out-think, out-maneuver, and out-fight any adversary under conditions of disruptive change"?[51] Or will we be like the French in 1940, who had none of those qualities and subsequently lost so overwhelmingly that their first battle became their last?

In 1946, General Eisenhower and Chief of Naval Operations Admiral Chester Nimitz established the Armed Forces Staff College in Norfolk, Virginia, to capture and teach the joint lessons of World War II—lessons that the Army and Navy (as well as the Air Force and Marines) learned the hard way in the Pacific, North Africa, and Normandy, and sadly have relearned in numerous campaigns since then. Eisenhower later commented that "separate ground, sea and air warfare is gone forever. If ever again we should be involved in war, we will fight it in all elements, with all services, as one single concentrated effort."[52] In the current era of Great Power competition that demands coherent policy and strategy and excellence in all-domain integrated operations, we can ill-afford to relearn the hard lessons that Eisenhower and Allied forces learned so expensively during Operation *Overlord* 75 years ago. We must not only continue to teach the joint lessons of World War II and other conflicts, but we must also improve our Service and joint readiness and prepare leaders from all Services to think, act, and behave jointly so that we can plan and execute the next *Overlord* with some anticipation of success. JFQ

Notes

[1] Figures from the U.S. Department of Veterans Affairs displayed by the National World War II Museum indicate that of the 16 million World War II veterans, fewer than 400,000 are alive in 2019, down approximately 100,000 from 2018. Available at <www.nationalww2museum.org/war/wwii-veteran-statistics>.

[2] Winston S. Churchill, *The Second World War*, vol. 6, *Triumph and Tragedy* (Boston: Houghton Mifflin, 1953), 10.

[3] Antony Beevor, *D-Day: The Battle for Normandy* (New York: Viking, 2009), 34, 36.

[4] See Rick Atkinson, *An Army at Dawn: The War in North Africa, 1942–1943* (New York: Henry Holt, 2002).

[5] See Carlo D'Este, *Bitter Victory: The Battle for Sicily, 1943* (New York: Harper Perennial, 2008); Rick Atkinson, *The Day of Battle: The War in Sicily and Italy, 1943–1944* (New York: Henry Holt, 2008). For a personal perspective of both Sicily and the airborne assault into Normandy, see James M. Gavin, *On to Berlin* (New York: Bantam Books, 1984).

[6] See Williamson Murray and Allan R. Millett, *A War to Be Won: Fighting the Second World War* (Cambridge, MA: Belknap Press, 2001), chapters 9, 13, 17.

[7] See Murray and Millett, *A War to Be Won*, 412; Beevor, *D-Day*, 36–37; and Carlo D'Este, *Decision in Normandy: The Real Story of Montgomery and the Allied Campaign* (New York: Penguin, 2004), 85, for similar opinions on German preparations.

[8] Winston S. Churchill, *The Second World War*, vol. 5, *Closing the Ring* (Boston: Houghton Mifflin, 1951), 582–583, 710–711; D'Este, *Decision in Normandy*, 29–30, 252–270; and Rick Atkinson, *The Guns at Last Light: The War in Northwest Europe, 1944–1945* (New York: Henry Holt, 2013), 15.

[9] Atkinson, *The Guns at Last Light*, 18, 21. U.S. forces alone occupied 1,200 camps and 133 airfields.

[10] The total force included 138 warships, 1,100 other combat ships, 4,200 landing craft, 221 escorts to protect the convoy, 805 cargo ships, and 59 obsolete craft to be used as breakwaters off of Omaha and Gold beaches. For example, a Landing Ship Tank could carry 20 Sherman tanks, 30 heavy trucks, 40 jeeps, and 350 men.

[11] Figures and information compiled from Atkinson, *The Guns at Last Light*, 15, 36–37; Murray and Millett, *A War to be Won*, 420; Craig L. Symonds, *Neptune: Allied Invasion of Europe and the D-Day Landings* (New York: Oxford University Press, 2014), 225–226, 305; and Ken Ford and Steven J. Zaloga, *Overlord: The D-Day Landings* (New York: Osprey Publishing, 2009). For a detailed description of landing craft, see Symonds, *Neptune*, 146–170.

[12] Beevor, *D-Day*, 92.

[13] For more on Field Marshal Percy Hobart's tank inventions, see Patrick Delaforce, *Churchill's Secret Weapons: The Story of Hobart's Funnies* (London: Robert Hale, 1998). For more on the DUKW, see the U.S. Army Transportation Museum, available at <www.transchool.eustis.army.mil/Museum/DUKW.htm>.

[14] Debate exists as to the cost-benefit of the Mulberries. Craig Symonds contends that the Allies transported just as much over the open shore at Omaha after the storm wrecked the American Mulberry as the British did using the Mulberry at Gold Beach/Arromanches. See Symonds, *Neptune*, 319–328. The British Mulberry provided service until Christmas 1944 when workers began dismantling it. For a succinct history, see Alain Ferrand, *Arromanches: A History of a Harbour* (Bayeux, France: OREP Editions, 2007).

[15] PLUTO and Red Ball Express info from Atkinson, *Guns at Last Light*, 240–241.

[16] Timeline and passage from Atkinson, *Guns at Last Light*, 32–36, 40. Atkinson does not mention the 4:30 a.m. final meeting, but it is confirmed in Symonds, *Neptune*, 240–242; and Dwight D. Eisenhower, *Crusade in Europe* (Baltimore: Johns Hopkins University Press, 1997). Salute and tears mentioned in Beevor, *D-Day*, 28. As Symonds (pg. 241) and others note, Eisenhower's decision was fortuitous as the storm that wrecked Mulberry A at Omaha Beach came on the evening of June 18 and lasted through June 22 and produced weather far worse than that of June 4–5. It is likely that had Eisenhower not launched the invasion, it would not have occurred under any of the conditions desired, at least not in June. This type of delay risked the entire plan as it would have been increasingly likely that the Germans would have picked up on the Allies' increased preparations as well as deduced the location. Moreover, with the V-1 attacks starting on June 12, it is possible that the Germans may have shifted their targeting from London and focused on the marshalling and port areas, causing, as Eisenhower stated, the invasion to be possibly "written off." Eisenhower, *Crusade in Europe*, 260.

[17] Symonds, *Neptune*, 284–289. Bradley confirms that he considered the diversion of follow-on forces. See Omar N. Bradley, *A Soldier's Story* (New York: Henry Holt, 1951), 220; Omar N. Bradley, *A General's Life*, with Clay Blair (New York: Simon & Schuster, 1983), 251. For current doctrine, see Joint Publication 3-02, *Amphibious Operations* (Washington, DC: The Joint Staff, 2019), available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_02.pdf>.

[18] Beevor, *D-Day*, 118.

[19] Ibid., 100–103; Atkinson, *Guns at Last Light*, 73–75; Ford and Zaloga, *Overlord*, 89.

[20] Atkinson, *Guns at Last Light*, 65–66.

[21] For strategists, the entire 26-page "Plan Dog" memorandum is worth reading. It is one of the most clear-eyed strategic assessments of the 20th century. It is referred to as "Plan Dog" because the option Stark recommended, with Army Chief of Staff General George Marshall's concurrence, was option "D" or "Dog." Emphasis in original. See Harold Stark, "Memorandum for the Secretary," Navy Department, Chief of Naval Operations, November 12, 1940, President's Safe Files, available at <http://docs.fdrlibrary.marist.edu/psf/box4/a48b01.html>.

[22] The other key strategic decisions were to begin limited offensive operations in the Pacific following the victories at Coral Sea and Midway, begin deliberate offensive operations against Japan, and invade Japan—this last decision made unnecessary by the Japanese surrender following the dropping of two atomic bombs in August 1945. For a short primer on all eight decisions, see Kent Roberts Greenfield, *American Strategy in World War II: A Reconsideration* (Malabar, FL: Krieger Publishing Company, 1982), 3–48.

[23] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 88, 605–608. For a thorough analysis of the integrated nature of policy, strategy, operations, and tactics, see Allan R. Millett, Williamson Murray, and Kenneth H. Watman, "The Effectiveness of Military Operations," *International Security* 11, no. 1 (Summer 1986), 37–71.

[24] While not the point of this article, the man, train, and equip tasks for all Services were immense and required creation from an almost dead stop. For example, the Army in 1939 numbered approximately 190,000 men. At its peak in World War II, it would reach 8.3 million. The 1940 draft and the beginnings of some rearmament as early as 1938 allowed the Navy and Army to begin to grow, but both departments would quickly become overwhelmed with the organizational requirements of fielding enormous ground, air, amphibious, naval, and air forces for a global war.

[25] See Richard Leighton, "U.S. Merchant Shipping and the British Import Crisis," in *Command Decisions*, ed. Kent Roberts Greenfield (Washington, DC: U.S. Army Center of Military History, 1960), 202, available at <https://history.army.mil/html/books/070/70-7-1/CMH_Pub_70-7-1.pdf>.

[26] Stalin was also pushing Roosevelt for relief from pressure following the German attack on Russia that began with Operation *Barbarossa* in June 1941.

[27] Atkinson, *An Army at Dawn*.

[28] Minutes, 81st Meeting of the Joint Chiefs of Staff, May 14, 1943, cited in Maurice Matloff, *Strategic Planning for Coalition Warfare, 1943–1944,* U.S. Army Center of Military History Pub 1-4 (Washington, DC: Government Printing Office, 1959), 131.

[29] Maurice Matloff, *Strategic Planning for Coalition Warfare, 1941–1942* (Washington, DC: U.S. Army Center of Military History, 1980), 156, available at <https://history.army.mil/html/books/001/1-3/CMH_Pub_1-3.pdf>.

[30] For more on the invasions of Sicily and Italy, see Atkinson, *The Day of Battle*.

[31] Operation *Overlord* was the codename for the overall invasion of Normandy from D-Day, the day of the first landing, until approximately D+90, when the Allies were to have expanded the beachhead, built up supplies and men, and pushed the Germans back to the Seine River. Operation *Neptune* was the codename for the all-important landing phase of *Overlord* in the Cotentin-Caen area.

[32] For the strategic direction, see Eisenhower, *Crusade in Europe*, 225. For an outline of the original three-division plan, its issues, and the changes made, see Albert Norman, *Operation Overlord: Design and Reality* (Westport, CT: Greenwood Press, 1970), 110–113; D'Este, *Decision in Normandy*, 55–70.

[33] In analyzing this portion of the operation, this paragraph purposely discusses five of the seven joint functions to show their interaction and interdependence. The other two are logistics and command and control.

[34] For more on Operation *Bodyguard* and Operations *Fortitude North* and *Fortitude South*, see Anthony Cave Brown, *Bodyguard of Lies* (New York: Harper & Row, 1975); Roger Hesketh, *Fortitude: The D-Day Deception Campaign* (New York: Harry N. Abrams, 2000); and Ben Macintyre, *Double Cross: The True Story of the D-Day Spies* (New York: Crown Publishers, 2012).

[35] Brown, *Bodyguard of Lies*, 660–662.

[36] Ibid., 690. Ultra decrypts indicated that Rommel appointed *General der Panzertruppen* Leo Baron Geyr von Schweppenburg to command the growing Panzer army in Normandy once assembled. This could potentially include the 1st, 2nd, 9th, and 10th SS Panzer Divisions, the 17th SS Panzer Grenadier Division, the 21st Panzer Division, and the Panzer Lehr Division. Accordingly, Montgomery decided to find Schweppenburg's headquarters and destroy it, which the Royal Air Force did on June 9. As James Gavin notes in *On to Berlin*, it was not hard to locate German senior headquarters. They were usually in a château surrounded by trees, and the roads leading into them had dugouts into the banks on the sides of the road for command and staff cars to park. It seems most Frenchman in Normandy in 1944 had bicycles, not motor vehicles. Gavin, *On to Berlin*, 87.

[37] Ibid., 647–648; Beevor, *D-Day*, 54.

[38] The best book on the glider raid on the twin bridges at Bénouville and Ranville is Stephen E. Ambrose, *Pegasus Bridge: June 6, 1944* (New York: Simon & Schuster, 1988).

[39] Brown, *Bodyguard of Lies*, 665–666.

[40] The Das Reich Division was particularly ruthless in dealing with French citizens and partisans. For more on the Das Reich Division and the French Resistance, see Beevor, *D-Day*, 165–167; and Max Hastings, *Das Reich: The March of the 2nd SS Panzer Division Through France* (New York: Henry Holt, 1982).

[41] Atkinson, *The Guns at Last Light*, 65, 68; Symonds, *Neptune*, 254–256, 266.

[42] Murray and Millett, *A War to be Won*, 419; Nigel Hamilton, *Master of the Battlefield: Monty's War Years 1942–1944* (New York: McGraw-Hill, 1983), 598, 623; and Bradley, *A Soldier's Story*, 221. For Corlett's opinion, see Charles H. Corlett, *Cowboy Pete: The Autobiography of Maj Gen Charles H. Corlett* (Santa Fe, NM: Sleeping Fox Publishing, 1974).

[43] Traditional artillery had a longer trajectory or arc that made it unsuitable for firing into the less than 8-foot-wide sunken cart paths where German gunners would hide. The small size of each field, usually no larger than 2 acres, meant that the friendly artillery observer calling in fire from the other side of the field had an equal chance of being hit by his own artillery. High-angle mortars were the preferred indirect fire weapon. Finally, the hedgerows themselves, measuring 1 to 4 feet wide and from 3 to 15 feet high, with thick roots and a tangle of branches and brambles, were formidable obstacles. For more on the *bocage* and U.S. Army efforts to adapt its tactics and technology to the terrain, see Michael Doubler, *Busting the Bocage* (Fort Leavenworth, KS: Combat Studies Institute, 1988), available at <www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/Doubler-Bocage.PDF>; and his *Closing with the Enemy: How GIs Fought the War in Europe, 1944–1945* (Lawrence: University Press of Kansas, 1994).

[44] Atkinson, *The Guns at Last Light*, 111; Beevor, *D-Day*, 252–253.

[45] Charles Cawthon, *Other Clay: A Remembrance of the World War II Infantry* (Boulder: University Press of Colorado, 1990), 76, cited in Atkinson, *The Guns at Last Light*, 111.

[46] See Doubler, *Busting the Bocage*, 4–5; *Closing with the Enemy*, 60; Beevor, *D-Day*, 242, 258. The 4th ID lost 2,400 casualties from July 6–24 after joining the fighting in the bocage. D-Day casualty figure from Atkinson, *The Guns at Last Light*, 85.

[47] The Périers Road (U.S. zone of attack) and Périers Ridge (British zone of attack) are two separate and distinct locations. Renie's 3rd Division attacked on a single brigade front with the 8th Infantry Brigade. The 185th Infantry Brigade was to pass through and attack toward Caen, supported by elements of the 27th Armored Brigade. Portions of the armored brigade became backed up on the beach as the tide moved in, delaying their arrival to pick up the infantry. The 9th Armored Brigade was held in reserve, but when landed was directed by Lieutenant General George Allen Crocker, the corps commander, to support the airborne forces in the vicinity of Pegasus Bridge. See D'Este, *Decision in Normandy*, 120–150.

[48] Ever since the failure to seize Caen on D-Day, Montgomery, some of his subordinates, and some military historians have argued that it was not Montgomery's intention to do so, but instead to pull all of the German armored forces in against the British near Caen so that the Americans could "break out." While that is essentially what happened *after* Montgomery failed to take Caen, it was not his original intent. D'Este categorically proves this point in *Decision in Normandy.*

[49] Montgomery finally succeeded in pushing beyond Caen in Operation *Goodwood*, July 18–20, 1944. The British Second Army began the battle with 1,370 tanks. It lost over 400 in the battle. The Germans had 230 tanks and 600 assault guns and lost 75 tanks or guns total. See Atkinson, *The Guns at Last Light*, 133–137. The Battle of Kursk in western Russia, July–August 23, 1943, was the largest tank battle of the war with approximately 3,000 tanks involved.

[50] The original reference was made by Arthur Wellesley, the Duke of Wellington, about his defeat of Napoleon at Waterloo. However, it has been used frequently by participants and several authors to describe the nearness with which Operation *Overlord* came to failure.

[51] Department of Defense, *Capstone Concept for Joint Operations 2030*, November 1, 2018, Classified, portion cited is unclassified, 1.

[52] Dwight D. Eisenhower, "Special Message to the Congress on Reorganization of the Defense Establishment," April 3, 1958, cited in the *New York Times*, April 3, 1958.

Aviation ordnanceman applies final wiring to GBU-24 laser-guided bomb attached to F-14 "Tomcat" fighter aircraft on board USS *Theodore Roosevelt* during *Allied Force*, Adriatic Sea, May 4, 1999 (U.S. Navy/Dennis Taylor)

Attacking Fielded Forces

An Airman's Perspective from Kosovo

By Phil Haun

The Dayton Peace Accords in 1996 settled the Bosnian civil war but left unresolved the ethnic conflict in Kosovo, the semi-autonomous region in southern Serbia. By 1998, clashes between Serbian police and ethnic Kosovar Albanians produced a humanitarian crisis only temporarily resolved by a U.S.-brokered peace agreement that quickly unraveled over the winter. Reinvigorated efforts at a peace deal failed at Rambouillet, France, in February 1999, however, and frustrated U.S. and North Atlantic Treaty Organization (NATO) leaders ultimately authorized three nights of restricted airstrikes to bring the Serbs back to the negotiating table. Serbia responded instead by launching an ethnic cleansing campaign that displaced hundreds of thousands of Kosovar Albanians. As a result, the air-only campaign, Operation *Allied Force* (OAF), extended for 78 days. A truly joint and multinational coalition effort, OAF involved hundreds of aircraft and thousands of Airmen and intelligence officers from the U.S. Army, Marine Corps, Navy, and Air Force, alongside those from other NATO nations.[1] The air tasking included strikes against leadership, economic, and infrastructure targets in Serbia and military forces in Kosovo. Ultimately, the strikes against fielded forces failed to convince Serbian president Slobodan Milosevic to withdraw his forces. Rather, his desire to remain in power and the threat posed by a continuation of airstrikes, which held hostage Serbia's stagnated economy, along with diplomatic pressure by

Dr. Phil Haun is the Dean of Academics at the U.S. Naval War College.

the Russians, compelled Milosevic to concede Kosovo.[2]

Controversy over the effectiveness of NATO air attacks against Serbian fielded forces was fueled in the final days of the war when U.S. military leaders claimed that half of the 300 Serbian tanks deployed to Kosovo had been destroyed.[3] General Wesley Clark, Supreme Allied Commander Europe, soon scaled back the battle damage assessment (BDA) to 110 tanks as NATO officials observed Serbian forces withdrawing with their armor in tow.[4] In response, Clark ordered a reassessment that, when released in September 1999, further reduced the count to 93 tanks hit, of which 26 were catastrophic losses and 67 were severely damaged.[5]

Yet the revision came too late. At the time, and to this day, it remains widely believed that the actual number killed was closer to the 13 tanks declared by the commander of the Serbian forces shortly after the withdrawal.[6] The final narrative from Kosovo depicted NATO airmen as incapable of identifying enemy ground forces as the Serbs hid and camouflaged their military vehicles, tricking pilots into attacking decoys and then making spurious claims.[7] Lost in this controversy was an understanding that the effectiveness of air operations against fielded forces should be measured not by the number of tanks destroyed, but rather by the degree to which airpower denied ground forces the ability to execute their preferred strategy and achieve their desired military and political objectives.

In May 2010, a decade after the NATO bombing of Yugoslavia during the Kosovo War, I had the opportunity to travel to Kosovo to investigate the accuracy of my mission reports. From March 31 to June 7, 1999, I flew 28 combat missions in Kosovo where I conducted 73 airstrikes as an A-10 airborne forward air controller (AFAC). I experienced firsthand the challenge of locating Serbian armor, particularly as the conflict extended and as the Serbs adapted to U.S. tactics. Flying above 10,000 feet above ground level to avoid Serbian antiaircraft artillery and infrared-guided shoulder-launched missiles, I observed Serbian troops appropriating civilian vehicles, which were off limits to airstrikes due to NATO rules of engagement (ROEs), and driving them from village to village to conduct ethnic cleansing. As the war progressed, I further observed the proliferation of decoys designed to absorb the attention and bombs of NATO airmen.

Right after the war, with the BDA controversy mounting, the U.S. Munitions Effectiveness Assessment Team was dispatched to Spangdahlem Air Base, Germany, in preparation for its deployment to Kosovo. There I provided the team with a detailed description of the tanks, armored personnel carriers (APCs), and artillery pieces I had attacked. Later, in September 1999, I was summoned to Brussels to be among a handful of NATO pilots to stand alongside General Clark when he released an updated BDA based on the team's findings.[8]

Eleven years later, while conducting research, I had the opportunity to travel to Kosovo where, aided by a Kosovar Albanian driver and translator, I visited six of my strike sites.[9] The number of sites was limited due to time constraints and safety concerns. Given these restrictions, several targets were selected near major roads and where target areas could be identified utilizing imagery available from Google Earth. At all target locations, local Kosovar Albanians were found who claimed to either have witnessed or have knowledge of the strikes. In eyewitness accounts, individuals recounted their memories of the target, attack, and battle damage. These accounts were then compared to my submitted mission reports. Overall, on airstrikes where I could visually identify targets, what was reported from the air was corroborated by witnesses on the ground. Unfortunately, this was not the case for the one strike where I had inferred target identification from other visual cues.

This article does not dispute the general claim of the ineffectiveness of NATO airstrikes against Serbian fielded forces in Kosovo.[10] A variety of factors made the systematic execution of such attacks problematic. Poor weather and rugged terrain are environmental factors that have and will continue to challenge air forces in prosecuting attacks. The lack of friendly ground forces to provide target identification and to prevent the Serbs from dispersing their forces would later lead to innovations by embedding joint tactical air controllers alongside indigenous friendly ground forces in Afghanistan and Libya. Challenges with untimely intelligence, surveillance, and reconnaissance (ISR) to conduct strikes on mobile targets would further spur investment in the near real-time intelligence provided by Predator and other remotely piloted aircraft. Similarly, onboard sensors on tactical aircraft proved inadequate for inflight target identification, which led to the development and widespread deployment of advanced targeting pods to most U.S. tactical aircraft. The lack of adequate doctrine and training for conducting direct strikes without coordination with friendly ground forces also limited airpower's effectiveness against fielded forces, a shortcoming that unfortunately has yet to be adequately resolved.

Instead of simply critiquing airpower's shortcomings in attacking fielded forces, this article draws on the author's experience in Kosovo to extract 11 generalizable lessons as to the challenges and requirements that remain for executing and assessing effective airstrikes against fielded forces. To do so, two of my airstrikes—one successful and one unsuccessful—are analyzed. These are first described based on the notes and mission reports I made immediately after the attacks in April and May 1999. Each strike is then reexamined from the ground perspective on the basis of interviews conducted in Kosovo in May 2010. As with the majority of the A-10 strikes during the war, both of the air attacks examined were conducted against Serbian military vehicles from medium altitude, during daylight, and under visual flight conditions.

The evidence is admittedly anecdotal and biased. Due to unexploded ordnance concerns, it proved impossible to examine strike sites away from major roads in the areas where the Serbs had deployed many of their decoys. In addition, the A-10 was designed, and its pilots specifically trained, for attacking ground forces. If any combat aviator should have been able to identify valid ground targets, it was an A-10 pilot. At the time, I was a highly experienced weapons instructor with 2,000 hours flying the A-10 in close air support and AFAC missions. Even so, experience goes only so far, and there were clear limits as to what could be observed from the air. Furthermore, target coordinates were imprecise as the A-10 did not yet have global positioning systems (GPS), and pilots relied instead on plotting targets in the cockpit from a stack of dated 1:50,000-scale maps designed for the Army. Moreover, the electro-optic (TV) and infrared LITENING targeting pods I would later employ in Afghanistan were not yet available. Instead, A-10 pilots relied on visual searches, augmented by commercially available 20-power, image-stabilized binoculars.

While these two airstrikes may not be representative of the overall experience of NATO airmen in Kosovo, when combined the strikes do provide a useful point of departure to consider the key attributes of effective air operations against fielded forces.

A Successful Mission: The Convoy

April 8, 1999: From the Air. My first AFAC mission over Kosovo was on March 30, but due to cloud cover, a condition typical of the Balkans in early spring, I could not conduct any airstrikes until April 8. I was the flight lead for a two-ship of A-10s assigned for AFAC duty. In the first of two assigned vulnerability periods, I controlled strikes on several military trucks parked in a compound in southwest Kosovo. During aerial refueling between vulnerability periods, I received a report from the Joint Surveillance Target Attack Radar System of a 50-vehicle convoy moving 8 miles west of Pristina. Upon returning to western Kosovo, I identified the convoy as a column of refugees. The radar system then relayed that a Predator unmanned aerial vehicle had spotted two APCs and a tank moving east near my position. Rolling the jet over, I visually identified beneath me a small convoy with one large and two small armored vehicles approaching a T-intersection in a little village. Extending to the north, I selected an infrared-guided air-to-surface Maverick missile and rolled in and locked up what I identified in the cockpit video to be a self-propelled artillery piece, a Russian 2S1 Gvozdika. Upon receiving indication of a valid lock, I launched the missile, then pulled up and rolled over to observe the weapon's impact. Once the rocket motor burned out, I lost sight of the missile and waited. Finally, the 2S1 burst into flames just before it reached the T-intersection. Sparks flew, and black smoke billowed, indicating a secondary explosion. My wingman then attacked one of the APCs, and before departing, I observed and strafed several tanks just north of the village. Debrief video review of the Maverick seeker confirmed the target likely to be self-propelled artillery.

May 18, 2010: From the Ground. My driver and interpreter, Zeka, drove west out of Pristina while I acted as navigator with a handheld GPS, an old flying map, and an aerial photo I had previously printed from Google Earth. We located the village and the T-intersection where I had plotted the strike. We parked in front of a nearby house, and two men in their mid-thirties approached us as we got out of the car. Zeka explained why we were there, and Ruzhdi and his brother Shkelza introduced themselves and motioned that we follow. As we walked, the men identified themselves as former Kosovo Liberation Army fighters who had been forced from their homes during the war, along with 8,100 Kosovar Albanians who had taken to the nearby forests while 2,000 Serbian troops had encamped in their village.[11]

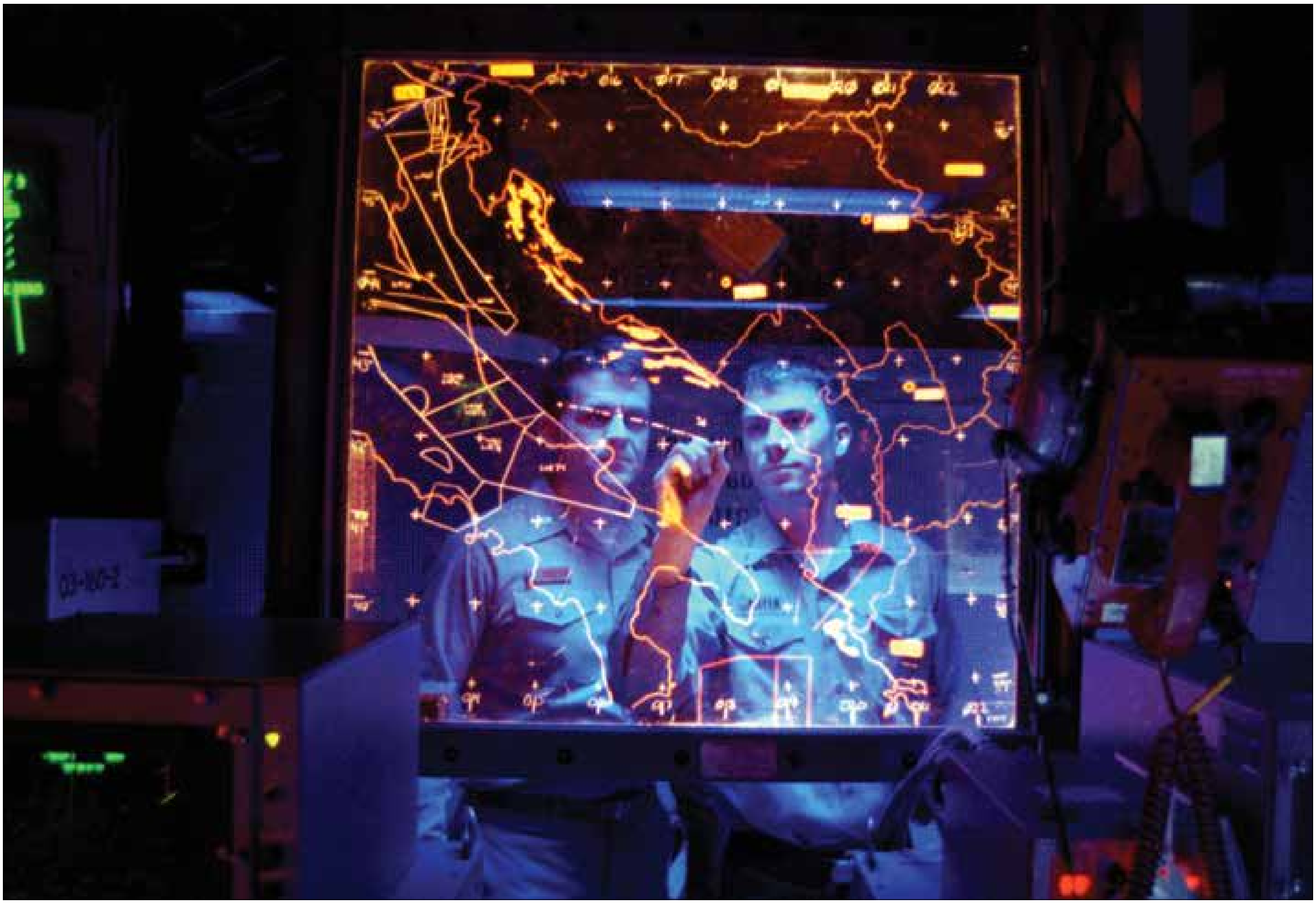
We walked down a narrow lane where shrapnel had left pockmarks in the walls of several houses. We entered a large yard with a farmhouse and a raised building with three parking spots underneath. Ruzhdi described how Serbian forces had quartered in the yard, using an upper room in the building for meals and storing their two APCs and a tracked artillery piece beneath.

When asked about the attack, Shkelza stated he had witnessed the strike from a field 3 kilometers to the southeast. He pointed up and to the north and recounted how an A-10 had shot a missile at the self-propelled artillery piece just as the vehicle was pulling out to follow the APCs. The large vehicle had been hit as it passed the back of the building, and secondary explosions had caused the damage to the walls of the houses we had just observed.

Ruzhdi added that 16 Serbs, including an infantry platoon catching a ride on top of the 2S1, had been instantly killed in the strike. A further 55 Serbs had been either killed or wounded from the secondary explosion.[12] The two brothers showed us the upper room, which had since been renovated, where they maintained soldiers had been eating at the time of the attack. In addition, Ruzhdi claimed that over the ridge a few kilometers to the north, the A-10s had also destroyed a tank, an armored vehicle, and three heavy trucks.

When asked what happened to the damaged vehicles, Ruzhdi stated that the self-propelled artillery piece had burned to the ground, leaving nothing to remove. The other vehicles had either been towed away by the Serbs or by KFOR, the NATO-led Kosovo Force, after the war. Before I left, Ruzhdi thanked me and related that after the strike that day, the Serbian forces had departed and the villagers were able to return to their homes.

Assessment of the Convoy. The April 8 airstrike was the only time in the war when I attacked a moving vehicle. The Serbian forces adjusted to having NATO aircraft overhead by operating at night or under cloud cover or by driving civilian vehicles. It was also the only time I received real-time target description and coordinates from a Predator. In this case, the eyewitness account from the ground matched what I had observed from the air, except for the additional information of the battle damage sustained from the secondary explosions. The only reasonable explanation for such a large blast would have been the detonation of artillery rounds the 2S1 stores internally.



Sailors review manual tracking procedures of target using plot board in Combat Direction Center at sea aboard USS *Theodore Roosevelt* in support of *Allied Force*, Adriatic Sea, June 3, 1999 (U.S. Navy/William L. Vandermate)

This attack highlights several lessons on the employment of airpower against fielded forces. First is a general reminder that when tactics prove successful, the enemy will quickly adapt. Rarely in Kosovo did the same tactics work for more than a few days. The enemy will address exposed vulnerabilities and adopt countermeasures as quickly as possible. Interaction with the enemy is dynamic, and tactics and doctrine must be flexible to evolve quickly in the battlespace where Darwin rules.

Second, when faced with the threat of credible airstrikes, ground forces disperse and hide. While such a response increases their survivability, such tactics may leave ground forces vulnerable to ground attack. In the case of Kosovo, however, Serbian forces did not face the credible threat of NATO ground troops. As a result, the Serbian army could continue conducting ethnic cleansing by abandoning their tanks and APCs, and by picking up their AK-47s and driving in confiscated Kosovar automobiles. The Serbian army was never forced to choose between concentrating against enemy ground forces and dispersing to avoid air attacks.[13]

Third, persistent ISR is critical for targeting fielded forces, and the Predator set the standard for ISR in Kosovo.[14] Its image-stabilized, magnified video camera provided an unmatched capability to locate and identify Serbian forces, and its feed to the Combined Air Operations Center at Vicenza, Italy, sped up the target approval process. The Predator flew lower, slower, and loitered longer over targets than any manned aircraft. As a result, it could visually identify targets where other ISR sensors could not. On one occasion, when I witnessed a Predator flying well below me, straight and level through a heavy volley of antiaircraft activity, I thought, "There goes the bravest pilot I've ever seen." Its relatively low cost and ability to operate without aircrew in the cockpit allowed the Predator to assume much greater risk.[15] Unfortunately, due to the high demand for Predator video, higher authority tasking, such as monitoring refugees, frequently superseded the targeting of fielded forces. The Predator was valuable but rarely available, and at the time it had not been fully integrated into tactical air operations.[16]

Fourth, as to BDA, after the war the tank count became the most important metric for measuring airpower effectiveness against the Serbian fielded forces. This measure, however, proved problematic. Theoretically, a highly effective air campaign against armor *should* have caused the Serbs to hide their tanks, which is in fact what occurred. The enemy's expectation of lethal airstrikes

Two U.S. Air Force A-10A Warthogs, from 52nd Fighter Wing, 81st Fighter Squadron, Spangdhalem Air Base, Germany, in flight during NATO Operation *Allied Force* combat mission, April 22, 1999 (U.S. Air Force/Greg L. Davis)

should deter them from risking their forces whenever it is not absolutely necessary. It is therefore impossible to determine by the number of vehicles destroyed whether airstrikes were effective. A low tank kill rate might indicate that the ground forces were deterred from using their armor, while a high tank kill rate might indicate that ground forces were more highly resolved to achieve their objective and undeterred by airstrikes.

To be clear, this article is not claiming that NATO airstrikes were effective against Serbian fielded forces in Kosovo but that the tank count was not an adequate measure. Airpower was ultimately ineffective against fielded forces because it did not stop Serbian ethnic cleansing operations, nor did the threat to fielded forces convince Serbia to withdraw from Kosovo.[17] Without the threat of a ground invasion, Serbs were free to conduct operations without risking their tanks, APCs, or artillery. The attrition rate of enemy armor, just like the body counts from Vietnam, is an inadequate measure of combat effectiveness. It is far more informative to ascertain whether military and political objectives are being achieved.

Fifth, an additional challenge to conducting BDA is in validating strikes. I reported most of my strikes as hits rather than kills, as I was reluctant to call a strike a kill unless I had observed a direct hit *and* secondary explosions.[18] Without the onboard sensors or confirmation from a ground-based joint tactical air controller capable of conducting precise post-strike BDA, a mission report was at best an informed guess.[19] After the war, the absence of destroyed heavy weaponry at strike locations was taken as evidence that pilot claims were exaggerated. As evidenced by the attack on the convoy, some damaged APCs, tanks, and trucks had been removed. It should not come as a surprise that the Serbs removed damaged equipment from the battlefield, as this is common army practice. There was ample opportunity to remove the equipment attacked early in the war. From an assessment of all the strikes I conducted throughout the war, only the vehicles and artillery attacked in the final days were abandoned by the Serbs.[20] Unfortunately, KFOR did not conduct adequate BDA forensics on the destroyed and abandoned vehicles hauled away. It is critical in future conflicts that BDA teams are prepared to gather data during the conflict from intelligence reports and then accompany ground forces into the combat zone to conduct the appropriate forensics as soon as possible.

This last lesson regarding BDA may now have been at least partially resolved by the development of more sophisticated sensors on tactical aircraft. In Afghanistan in 2004, I flew A-10s modified to carry the LITENING II targeting pod, which included enhanced electro-optics and infrared imaging. The optics on this sensor were so refined that, even from medium altitude, I could often distinguish an individual walking along a trail as being either a woman or a man just by their gait. Continued improvements in sensors will allow for more opportunities to validate BDA by strike aircraft.

The Unsuccessful Mission: The Barn

May 12, 1999. On May 11, a Predator had spotted 20 Serbian military vehicles as they were being moved into a large L-shaped building. A two-ship of A-10s from my squadron had subsequently strafed the building and reported secondary explosions accompanied by an unidentified pale yellowish-green smoke. That evening I discussed the specifics of the attack with the pilots and made a mental note to look for similar buildings where there might also be armor. During the next day's intelligence briefing, I noted the villages where Serbian tanks had recently been reported.

While searching a small village in southeast Kosovo, I identified a 200-foot-long metal building, which I judged to be a barn, near the village of Viti. Mud tracks made by heavy equipment led from a group of freshly dug, large earthen berms to the barn. The empty berms resembled the revetments the Serbian tanks used in prepared defensive positions along the border. I radioed a description of the building, the berms, and the accompanying muddy tracks before departing for the tanker. While aerial refueling, I received permission from the CAOC to attack the building. I then coordinated for strike aircraft.

Returning to the area, two Turkish F-16s checked in. I talked them onto my position and when they called visual, I rolled in and marked the barn with two 500-pound bombs, one of which was a direct hit. Climbing off target, my wingman called "break" and as I jinked, I could see the distinctive tiny red muzzle flashes of small-arms fire and the white-gray airbursts from antiaircraft activity as it popped off below my jet. The F-16s followed my attack, dropping their ordnance, after which I noted the barn on fire with an accompanying pale yellowish-green smoke.

May 17, 2010. Eleven years later, the "barn" was the last stop on the first day visiting strike sites. As the car turned into the driveway of an older two-story farmhouse, I noticed the house was attached to a long single-story building with a new red roof. A man greeted us, introducing himself as Sherife, the son of the owner of the farm, Habib. Sherife explained that during the war, Serbian forces had been deployed in their village. When asked about the airstrike on May 12, 1999, he confirmed the earthen berms to have been military and the tracks were made by Serbian tanks kept in the barn. The local Serbian troops, however, had left the farm the day prior to the attack.

Sherife appeared happy to talk with us and invited us into the farmhouse to meet his mother. Habib was also in the house but we were told he was on his deathbed. Sherife's mother insisted on making coffee while explaining how she had sent Sherife out of Kosovo the week before the strike, after he had been severely beaten by local Serbian troops. She and Habib had remained behind to care for the farm and, once the Serbs had removed their tanks, the two had moved their tractor and car, along with 60 head of sheep into their barn for safekeeping.

She and Habib were in the house attached to the barn when the first bomb hit. They ran into the woods and watched as the barn burned with everything inside destroyed. Fortunately, the house had been spared. As she spoke, Sherife reappeared with Habib, who insisted on greeting me. Though unable to speak, Habib sat next to me and held my hand as his wife continued the story.

The family held no grudge against the destruction of their property as NATO had been fighting the Serbs for Kosovo's freedom. Instead, every year the family celebrates May 12 as the day NATO bombed their farm. For many years, the U.S. Army commanding officer from nearby Camp Bondsteel visited the house on the anniversary of the strike out of respect for the family. She pulled out a certificate presented on one such occasion. When asked about the yellowish-green smoke, she just shrugged.

Assessment of the Barn. For over a decade, I believed the barn to be a successful attack. I was surprised to find that instead of destroying Serbian armor, I had caused collateral damage and endangered the lives of two civilians. From this unfortunate strike, five additional lessons can be distilled.

Sixth, there is no substitute for direct target identification. In this case, I had relied on indirect visual indications. The fact that the Serbs had been observed hiding their vehicles in similar buildings had motivated the search, request, and approval for the strike. In addition, intelligence had indicated Serbian armor in the village, which is why I searched in that particular location. The earthen berms further indicated military vehicles were being used at the location, and the muddy tracks leading to the barn indicated the Serbs were utilizing the barn to hide their armor. None of these indications was wrong. As this strike demonstrates, however, there is no substitute for real-time, direct target identification. The greater the reliance on indirect measures for target identification, the more chance a strike goes wrong.

Seventh, realize that there are no fixed targets. Aircrew and intelligence officers have long distinguished between fixed and mobile targets. This is a mistake; although structures may not move

Supreme Allied Commander Europe General Wesley Clark meets with members of 510th Fighter Squadron and 555th Fighter Squadron deployed to Aviano Air Base, Italy, on May 9, 1999, in support of Operation *Allied Force* (U.S. Air Force)

in the three spatial dimensions, their function can change rapidly in the fourth dimension of time. The timeliness of intelligence for structures is as important as it is for fielded forces. In this case, the building transformed overnight from a Serbian armor vehicle storage facility to a sheep barn. Those who continue to distinguish between fixed versus mobile targets ignore the fact that targets can maneuver within both time and space.[21]

Eighth, the validity of intelligence is based on its timeliness, origin, and form. Intelligence reports older than 6 hours were unlikely to result in a successful airstrike. Intelligence was most effective when delivered quickly and in a medium closest to how it was intended to be employed. For daylight operations, this meant timely photos with sufficient detail of the surrounding area for the pilot to be able to locate the target from the air. If a photograph was taken the previous day, the vehicle may have long since been moved or the function of a building may have changed. While intelligence might be useful for building situational awareness, information without accompanying recent photographs would not directly lead to a strike, and it still remained up to Airmen to locate and identify valid targets.[22]

Ninth, it was the threat from Serbian air defenses, not ROEs, that restricted operations to above 10,000 feet above ground level. Combat effectiveness depended on the ability to attack enemy forces, which required the time to be able to locate and validate targets. The threat of Serbian air defenses, however, compelled operations to medium altitude. When operating at lower altitudes, I had to maneuver constantly to avoid ground fire, which in turn prevented time spent searching for targets. As the war progressed, I circled higher and higher, well above the ROE hard deck, which allowed more heads-down time to search for new targets and less time spent worried about Serbian air defenses. The ROE reflected the desire by senior air commanders to limit exposure. In Kosovo, it was not ROE restrictions but the enemy threat that limited combat effectiveness.

Tenth, air operations are dramatically affected by lighting and weather conditions more so than typically acknowledged. Nighttime operations were far less effective than daytime operations as sensors were not capable of target identification at night, a limitation the F-16 AFACs encountered with their LANTIRN (low-altitude navigation and targeting infrared for night) targeting pods.[23] Furthermore, cloud cover through mid-April prevented medium altitude operations. The inability to validate targets without visual identification, coupled with concerns over collateral damage, precluded dropping bombs through clouds. Often ignored in general discussions on airpower effectiveness is the impact weather can have, a point largely overlooked in the recent air campaigns in the desert climates of Iraq, Afghanistan, Libya, and Syria. Weather had, however, significantly restricted airpower operations over Germany, Japan, Korea, Vietnam, and Bosnia, as it did in Kosovo, and should be taken into account as a primary consideration for employing airpower in future conflicts.

Eleventh is the issue of decoys. The Serbs, like many armies, deployed decoys as part of their tactics. The use of decoys did not make the Serbian army exceptional, nor were NATO airmen necessarily naive for striking them. At medium altitude, it is difficult to discern a decoy from a valid target. The method often employed was not to be overly concerned about differentiating between the two, but to strike any targets located. If the target disappeared when struck, it was likely a decoy. The point is that when targets are rare and weapons plentiful, it is preferable to waste some bombs on decoys rather than allow valid targets to escape. At the end of the war, the fact that destroyed decoys were found or that derelict hulks in the open had been struck multiple times proved neither the brilliance of Serbian tactics nor the naiveté of NATO airmen. It instead revealed the shortcomings of some analysts who reached broad conclusions over the ineffectiveness of airpower based on the anecdotal evidence of these individually ineffective airstrikes.

This is not to say that decoys do not provide challenges for air operations. Given the increased reliance on a limited number of relatively costly precision-guided weapons, along with lessons from the recent air campaign against the so-called Islamic State, where weapons availability became an issue, the impact of decoys on the efficient utilization of ordnance may be a concern in future operations.

The Kosovo War was a unique conflict fought two decades ago. It would be easy to ignore its lessons as specific to that war or nullified by new technologies and doctrines or contradicted by lessons from other conflicts. That would be a mistake. Airmen have now largely solved the problem of how to place a weapon on a target, but challenges remain of first being able to locate and identify targets as valid and then being able to determine the effect of strikes on the targets that are attacked. This article has identified enduring challenges of attacking fielded forces that will likely be present in the next conflict and are therefore worthy of consideration now.

In combat, the enemy will continue to adapt, and the joint force must be prepared for this eventuality with the organizations and doctrine to respond quickly to the inevitable changes required to succeed. Target identification will continue to be the major challenge for attacking fielded forces, which requires continual investment in real-time ISR systems not only to provide target identification but also to conduct high-quality battle damage assessment. Air forces can be potent but, just like land, sea, space, and cyber forces, each military instrument of power has its limitations. Airpower remains constrained by environmental factors of bad weather, poor lighting, and rugged and urban terrain as well as operational factors of enemy threat level and the absence of friendly ground forces. Finally, military commanders must be prepared to respond to misinformed measures of military effectiveness such as tank counts and destroyed decoys and instead redirect the discussion toward measures that more closely link military operations to the achievement of strategic objectives. JFQ

Notes

[1] The U.S. Army deployed Task Force Hawk consisting of attack helicopters and the Army Tactical Missile System (ATACMs) to Tirana, Albania. Though Task Force Hawk never employed its helicopters or ATACMs in combat, its AN/TPQ-36 and-37 Fire Finder radars were deployed along the border to locate Serbian artillery positions.

[2] Phil Haun, *Coercion, Survival, and War: Why Weak States Resist the United States* (Palo Alto: Stanford University Press, 2015), 114–133; and Daniel Lake, “The Limits of Coercive Airpower: NATO’s ‘Victory’ in Kosovo Revisited,” *International Security* 34, no. 1 (Summer 2009), 83–112.

[3] Steven Myers, “Damage to Serb Military Less than Expected,” *New York Times*, June 28, 1999.

[4] William Arkin, “Operation Allied Force: ‘The Most Precise Application of Air Power in History,’” in *War Over Kosovo: Politics and Strategy in a Global Age*, ed. Andrew Bacevich and Eliot Cohen (New York: Columbia University Press, 2001), 25.

[5] James Diehl and Charles Sloan, “Battle Damage Assessment: The Ground Truth,” *Joint Force Quarterly* 37 (2nd Quarter 2005), 59–64.

[6] Rebecca Grant, “True Blue: Behind the Kosovo Numbers Game,” *Air Force Magazine* (August 2000), 74–78.

[7] Richard Norton-Taylor, “How the Serb Army Escaped NATO,” *The Guardian*, March 8, 2000.

[8] General Wesley K. Clark and Brigadier General John Corley, press conference on the Kosovo Strike Assessment, North Atlantic Treaty Organization (NATO) Headquarters, September 20, 1999, available at <www.nato.int/kosovo/press/p990916a.htm>.

[9] Haun, *Coercion, Survival, and War.*

[10] Stephen Hosmer, *The Conflict Over Kosovo: Why Milosevic Decided to Settle When He Did* (Santa Monica, CA: RAND, 2001), 77–90.

[11] I cannot vouch for the accuracy of the information. Every man I spoke to in Kosovo told me they were in the Kosovo Liberation Army. The small village did not appear to hold 8,100, but there were several villages in the area that combined could have housed that many. I also cannot vouch for 2,000 Serbian forces, which would have been too many for the one village, but could have been spread throughout the region.

[12] The author remains skeptical of the reported casualty figures. Though these were the numbers provided, they may have been inflated, particularly based on the relatively low level of observable damage to the building.

[13] The only exception was a brief period near Mount Pastrik in southwest Kosovo at the end of May.

[14] The Predator had not yet been armed with Hellfire missiles. By contrast, other intelligence, surveillance, and reconnaissance platforms that relied on synthetic aperture radars or moving target indicators did not prove to be effective as they could not provide positive target identification.

[15] NATO lost 25 unmanned aerial vehicles during the war. See Benjamin Lambeth, *NATO’s Air War for Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND, 2001), 97.

[16] I also found this to be the case in combat operations in Afghanistan in 2004. Efforts to coordinate tactics between A-10s and Predators in theater were continuously disrupted by higher headquarters tasking. As a result, combined tactics, such as the Predator providing laser designation for a laser-guided bomb dropped from an A-10, could not be exercised. This was particularly important since the first time such a combined tactic would have been employed would have been for a high-value target.

[17] Haun, *Coercion, Survival, and War,* 125–131.

[18] This only occurred three times: the strike just described, on an April 16 attack against a T-72, and on a June 7 attack on a T-54.

[19] The problem with the Maverick was that video was severed once the missile departed the aircraft. The problem with targeting pods is that the video is taken at aircraft altitude. There are some weapons, such as the GBU-15, that transmit weapons video to the cockpit up until weapons impact.

[20] I was able to validate battle damage for strikes on June 7 from photographs taken by NATO helicopters.

[21] A more infamous example was the attack on the Al Firdos bunker outside Baghdad on February 13, 1991, which at night served as an air raid shelter.

[22] Once I began flying with GPS and advanced targeting pods, accurate coordinates became more useful but were still not a substitute for a photograph.

[23] The challenges of night operations have been somewhat offset by the development of advanced targeting pods, which make clear-weather night tactics much more effective.

Marine with 3rd Battalion, 7th Marine Regiment, 1st Marine Division, scales wall during counter-IED training at Marine Corps Air Ground Combat Center, Twentynine Palms, California, July 25, 2019 (U.S. Marine Corps/Colton Brownlee)

Countering Threat Networks to Deter, Compete, and Win

Competition Below Armed Conflict with Revisionist Powers

By Vayl S. Oxford

The current geopolitical environment is the most complex, dynamic, and dangerous the United States has ever faced. During the Cold War, the Nation squared off against a superpower rival in the Soviet Union, and since its collapse, the United States has battled an assortment of rogue regimes and violent extremist organizations (VEOs). While rogue regimes and VEOs remain a threat to U.S. and allies' security, the United States must also contend with the threat posed by not one but two major state competitors, China and Russia, each fielding significant nuclear and conventional forces.[1] The 2018 National Defense Strategy directs the Department of Defense (DOD) to focus on "long-term, strategic competition" with these two "revisionist powers," whose regional and global ambitions are at odds with those of the United States and its allies, while also continuing to keep rogue regimes and VEOs at bay.[2]

Vayl S. Oxford is Director of the Defense Threat Reduction Agency.

As a Department, we are well versed in deterring state adversaries from initiating major armed conflicts against ourselves or our allies by maintaining nuclear and conventional forces capable of imposing severe costs against overt, direct military aggression by any state actor. However, the scope of the threat posed by revisionist powers extends well beyond these types of hostilities. While the United States must continue to seek cooperation with Russia and China in areas where our interests align, we must also recognize those areas where Moscow and Beijing seek to challenge U.S. military primacy and undermine the Nation and its allies. In such cases, the United States must be prepared to counter a broad range of malign activities carried out below the threshold of state-on-state armed conflict. These global threat networks can include leveraging rogue states, VEOs, and witting and unwitting actors in the private sector. To counter the efforts of revisionist powers to exploit the competition continuum between war and peace, we must recalibrate existing tools and approaches—including those initially developed after 9/11 to counter VEOs—in order to regain the initiative in the present era of Great Power competition.

The Defense Threat Reduction Agency (DTRA), which I have the honor to lead, is the DOD combat support agency responsible for enabling the Defense Department, the U.S. Government, and our international partners to counter and deter transregional and multidomain weapons of mass destruction (WMD) and improvised threat networks.[3] In this capacity, DTRA plays a key role in ongoing U.S. efforts to illuminate and dismantle VEO threat networks. As DOD refocuses on the long-term challenge posed by revisionist powers, I believe it is critically important to consider applying the best practices and lessons learned from combating nonstate networks to similarly uncover and counter the covert and deniable machinations of state actors and their global networks. These revisionist powers employ their own networks and exploit the networks of other state and nonstate entities. Applying our countering threat networks toolkit to reveal and stymie revisionist power activities across the conflict continuum is an important component of broader efforts to compete with Beijing and Moscow below the level of armed conflict.

This article describes the competition continuum and illustrates some of the actions of Russia and China within this space, identifies tools and approaches first developed to counter nonstate threat networks that can be adapted to counter revisionist powers and their global threat networks across the competition continuum, and discusses the potential benefits and possible risks of the United States pursuing these courses of action.

Competition Continuum

U.S. security is underpinned by a robust, flexible nuclear deterrent and powerful conventional forces. These capabilities deter potential adversaries from launching direct attacks against the United States due to the certain and severe costs Washington can impose in response.

Nuclear deterrence and conventional forces, however, cannot forestall all forms of aggression. Moreover, the current threat environment is described as a world of long-term competition that is exacted through a combination of cooperation, competition below armed conflict, and armed conflict.[4] While state adversaries seek to avoid direct armed conflict with the United States, revisionist powers have shrewdly calculated the thresholds below which they can operate to further their own interests—often at the expense of the United States or its allies—without triggering an automatic U.S. military response. General Joseph Votel, former commander of U.S. Central Command, described this "gray zone" between peace and armed conflict as a space "characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."[5] Russia and China view the United States as the principal obstacle to realization of their regional and global ambitions. Both revisionist powers operate across the competition continuum as part of a broader, ongoing campaign to undermine U.S.-led alliances and regional security arrangements, erode U.S. global power and leadership, and challenge the rules-based international order. These efforts include several components.

Covert, Deniable Hybrid Operations. Russia used military forces operating without clearly identifiable national military markings as part of its illegal seizure and annexation of Crimea, deploying these forces across Ukraine's borders while denying its direct military involvement.[6] These "little green men" provide Russia a covert means to seize key targets or stir up internal dissent as a pretext for military intervention.[7] Similarly, China has deployed a supposed "fishing fleet" of ships in the Western Pacific that operates as a shadow maritime militia.[8] These vessels often loiter near disputed areas, harassing the maritime craft of other nations as part of China's broader effort to force other parties to drop their claims to reefs, islands, and waters. In both cases, these forces allow Moscow and Beijing to pursue key national objectives while simultaneously denying responsibility. Even if improbable, these denials can complicate efforts to attribute their involvement and organize a response.

Use of WMD for Assassination on Foreign Soil. With the attempted assassination of Sergei Skripal in Salisbury, United Kingdom, in March 2018,[9] Russia demonstrated its willingness to use advanced chemical weapons on the soil of a North Atlantic Treaty Organization (NATO) member.[10] In conducting the attack, Moscow violated the Chemical Weapons Convention, showed contempt for international norms, and demonstrated that it is prepared to employ a sophisticated WMD with little consideration of collateral damage. Moreover, in its efforts to hinder an international investigation by the Organization for the Prohibition of Chemical Weapons, Moscow was joined by Beijing, which often shares Russia's general opposition to greater international transparency or accountability.[11]

Supporting Nonstate Proxies. Russia has embraced the use of nonmilitary actors, such as private security companies, to advance its interests. These mercenaries (often former Russian military personnel) remain involved in the ongoing Ukrainian conflict and participated in an ill-fated February 2018 attempt to attack a combined Kurdish and U.S. force engaged in anti–Islamic State (IS) operations in Syria.[12] Similar to little green men, private military companies can operate below the threshold of state-on-state armed conflict while the Kremlin publicly denies involvement.

Enabling/Failing to Prevent Proliferation of Weapons and Sanctions Enforcement. Russia and China have a decidedly mixed record regarding the proliferation of weapons or dual-use items (goods or technologies that can have civilian or military applications), including items associated with WMD or improvised threats. The State Department, for example, has reported that China continues "to supply missile programs of proliferation concern" and that Russia remains engaged in dual-use activities that raise questions regarding its compliance with the Biological Weapons Convention.[13] In addition, terrorists and insurgents building improvised explosive devices (IEDs) in Syria, Iraq, and Afghanistan regularly procure items from both countries, including fertilizer purchased from Russian suppliers and electronic components purchased from Chinese suppliers.[14]

More broadly, Russia's and China's enforcement of sanctions against bad actors—including states illegally pursuing WMD and their delivery systems (or seeking to sell them)—is often lax. This is sometimes due to a lack of capacity to enforce sanctions; in other cases, it reflects a deliberate decision to deprioritize enforcement or allow these activities to continue. The United States, for example, has provided Beijing with photographic evidence of North Korean ships illegally loading petroleum from vessels (registered to third nations) just off China's coastline, well within an area where Chinese naval or coast guard craft should challenge and halt these types of transfers. Russia has also allowed similar practices, and both Beijing and Moscow have blocked efforts at the United Nations (UN) to publicly report these violations,[15] reducing the effectiveness of UN sanctions against Pyongyang.[16]

Challenging, Breaching, and Infiltrating Sovereign Boundaries (Land, Sea, and Air). Despite frequently emphasizing the importance of sovereignty to deflect criticism of internal activities, Russia and China have increasingly challenged sovereign boundaries in the land, sea, and air domains. As noted, Russian little green men infiltrated Ukrainian territory, leading several NATO members and partners that border Russia to step up efforts to secure their borders and monitor Russian military activity near their territories. Moscow and Beijing have also engaged in the provocative behavior of sending military aircraft and ships on patrols or excursions that are violations or near violations of U.S., allied, or partner airspace or waters. U.S., British, and Japanese aircraft, for example, have scrambled to intercept Russian bombers that have entered national airspace or air defense identification zones; the Japanese government reported conducting nearly 1,000 of these intercepts against Chinese or Russian aircraft in the past year.[17] In addition, in the last 2 years, Japan, Vietnam, and the Philippines have charged China with violating their territorial waters, using ships to engage in provocative, dangerous behavior that has resulted in the collision and sinking of vessels (as well as many near misses).

It is clear from these examples that Beijing and Moscow are engaged in a broad range of activities below the threshold of state-on-state armed conflict to challenge the United States and its allies in a manner that they believe will not result in a U.S. military response. In order to meet this challenge, the United States can draw on the lessons learned from countering nonstate threat networks in Iraq, Afghanistan, and around the world. For all their important differences, state and nonstate actors seeking to do harm to the United States and its allies employ similar means, and several of the tools honed during 18 years of battling terrorists and insurgents have utility in shedding light on, and pushing back against, Russia and China across the competition continuum.

Countering Threat Networks

The U.S. military developed its current concept of threat networks in the years after 9/11 due to a recognition that many of the insurgents and terrorists encountered by U.S. and coalition forces were not confined by borders or rigid state or bureaucratic structures.[18] These threat networks usually sought to remain hidden from view, eschewing uniforms or other identifying characteristics in order to blend in with civilian populations. Many had links or ties with communities across state borders that allowed them to recruit additional members and draw financial support from multiple sources. In many cases, they also cultivated transnational supply chains, including legitimate businesses unaware of the intended end use of their products.

In response, the U.S. Armed Forces developed a methodology and strategy for countering these nonstate threat networks that combined aspects of military engagement, security cooperation, and deterrence to apply steady pressure while disrupting their direct and indirect sources of support.[19]

Threat Network Illumination. To target threat networks, the totality of the network must be understood—including the relationships that allow them to operate. Numerous tools and skill sets are levied against the network, coupled with specialized U.S. human capital and partner nation governments and agencies. When effectively collected and assessed, this information sheds light on a threat network's internal and external relationships and reveals key nodes (such as their leadership and critical enablers). As David Richard Doran notes, "Understanding how adversaries use threat networks globally to compete with us below the threshold of traditional armed conflict is a critical first step to identifying opportunities" to mitigate their effects. This detailed picture of a threat network informs actions to exploit, disrupt, or degrade the network and ultimately scatter or collapse the larger interconnected structure.[20]

Ukrainian soldiers decontaminate vehicles as part of simulated chemical exposure event during field training exercise portion of Rapid Trident 2019, September 24, 2019, near Yavoriv, Ukraine (U.S. Army National Guard/Amanda H. Johnson)

Teaming to Defeat Networks. In many cases, however, the illuminated threat network reveals a complex entity with links and nodes across multiple jurisdictions and borders. To disrupt and defeat such networks, we must build teams across DOD, its U.S. Government partners, and with foreign counterparts to bring together the expertise, capabilities, and authorities necessary to isolate and take action against key network nodes. As Admiral Kurt Tidd, former commander of U.S. Southern Command, noted in March 2018, in order to combat nonstate threat networks that can include "drug traffickers, human smugglers, terrorist supporters, arms dealers and money launderers," it is vital for the U.S. Government to "integrat[e] our expertise and tools with those of committed [foreign] partners to remain more adaptive and capable than adversaries who exploit or target our citizens."[21] Dismantling a network may require, for example, combined operations by the United States and allied and partner governments, to include financial, customs, law enforcement, and military task force activities that starve VEOs of resources, prevent them from adding recruits, uncover their weapons caches and hideouts, and allow for the apprehension and prosecution or elimination of their leadership. In many cases, DOD is in a supporting role to an interagency or international partner that has the placement and authority to take the actions that maintain or achieve U.S. objectives.[22]

DTRA and its U.S. Government and international partners have worked hard to illuminate the activities of nonstate threat networks and assemble combined teams to counter the multifaceted challenge posed by this type of adversary. This experience, described in two case studies below, provides tools and templates that can prove valuable to countering malign activities short of armed conflict by major powers that employ similar methods.

Developing a Toolkit to Illuminate Threat Networks

Beginning in 2003, U.S. forces began encountering IEDs on the roads and highways of Iraq and soon thereafter in Afghanistan. These low-cost devices were soon inflicting injuries, causing fatalities, and slowing operations by U.S. forces deployed across both countries.[23] The U.S. Army responded to this threat by forming a task force, the Joint IED Defeat Organization, which evolved over time to become a core mission of DTRA.

Early U.S. Government efforts to counter IEDs struggled to assess large volumes of information collected from multiple sources on insurgents, the types of attacks carried out, and the variations of explosive devices employed. In addition to the challenge of sifting through mountains of data, different stakeholders faced serious technical challenges when they attempted to share this

Marine dresses in chemical, biological, radiological, and nuclear defense gear for sensitive site exploitation training during exercise Eager Lion 2019 in Jordan, August 27, 2019 (U.S. Marine Corps/Rhita Daniel)

information with each other. In response, U.S. Government teams developed cutting-edge analytical tools to integrate hundreds of data sets from previously disparate platforms and partners. DTRA continues to work hand-in-glove with its U.S. Government partners to enable information-sharing and continue integration of new data sets to further improve the fidelity of analyses of VEO strategies, tactics, and day-to-day operations. These teams also pioneered processes bringing together regional and functional subject matter experts directly with programmers in order to tailor existing tools to meet unique requirements. This nimble approach to metadata analytics helps DOD keep pace with threat networks that constantly adapt in response to U.S., allied, and partner actions against them.

All the tools described above improve U.S. commanders' situational awareness and ability to execute decisive actions against a threat network's key nodes. In the IED and improvised threat space, DTRA's flexible, evolving toolkit has provided timely and actionable assessments to effectively target key nodes associated with VEO improvised threats in Iraq, Afghanistan, and Syria.

Building Regional Partnerships

The devastation and chaos of the Syrian civil war pose an ongoing threat to regional security and stability, including several U.S. partners and allies. In addition to representing an acute humanitarian crisis, this flow of people raises a host of security concerns for nearby states, one of which is preventing VEO fighters and weapons—including chemical weapons or precursors—from leaving Syria. At various stages of the country's civil conflict, the security of Syrian government stocks of chemical weapons was in doubt, raising the possibility they could be seized by a terrorist organization or fall into the hands of an enterprising smuggler. In addition, IS's success in developing its own chemical weapons prompted fears it might attempt to remove these weapons from Syria to conduct attacks on U.S. allies or partners in the Middle East or further abroad.

Based on these threats, the United States, together with key allies such as the United Kingdom, partnered with Jordan and Lebanon to better protect their borders and prevent bad actors from smuggling chemical weapons, precursor materials, or other WMD-related items into their countries. Meeting this objective required a comprehensive, around-the-clock monitoring of borders that run along rough terrain, often in remote areas far from existing infrastructure. Operationally, smugglers and IS fighters needed to be distinguished from civilian refugees, while weapons, dual-use items, and other improvised threat materials needed to be detected and identified. The scope of the challenge required developing innovative, purpose-built "hardware and software" solutions for each partner state that brought together best practices from multiple actors, from local border guards to British military trainers and U.S. information technology engineers.

In Jordan, DTRA played a central role in orchestrating and developing the Jordan Border Security Program, which to date has provided a layered defense across more than 400 kilometers of border.[24] The program, which will soon fully transition to the Jordanian government, has taken a holistic approach to countering the threat of potential WMD proliferation through enhanced border detection and response capabilities. Physical barriers are provided where appropriate, while improved situational awareness is supplied by a network of watch towers equipped with sensors, radars, and other surveillance technology. Information streams are connected to battalion-, brigade-, and national-level operations centers, where they can be combined with other data or assessments that allow Jordanian authorities to quickly determine which resources to deploy to mitigate a threat. In circumstances where border personnel suspect the presence of a possible WMD or chemical, biological, radiological, or nuclear material, the program has also equipped and trained specialized mobile units to quickly respond and conduct an initial assessment of the potential WMD threat. Tying all this technical equipment and know-how together is a set of robust training programs for Jordanian border, law enforcement, military, technical, and disaster response personnel, as well as an equipment repair facility to ensure Jordanian officials can sustain the system's operations. Similarly, DTRA has partnered with Southeast Asian nations to improve the security of their maritime domains against WMD trafficking by nonstate actors, as well as trafficking by rogue regimes such as North Korea and Iran.

These projects have significantly enhanced the capacity of key U.S. partners to detect and interdict WMD and related materials at their borders. This WMD-focused assistance has broader second-order effects, improving these partner nations' overall border security and aiding their capabilities to apprehend VEO members and sympathizers and to identify and intercept conventional weapons. Critically, these combined U.S., allied, and partner teams provided the dynamic collaboration required to counter threat networks in and around Syria as well as trafficking networks in the South China Sea and nearby waters. As the National Defense Strategy emphasizes, this bolsters U.S. partnerships in parts of the world where revisionist powers are eager to exert malign influence through regional partnerships at the expense of U.S. objectives.

Application to Great Power Competition

State and nonstate actors differ in many critical ways, including the scale and scope of resources available to pursue their objectives. The methods utilized to counter nonstate threat networks, however, can provide a way ahead for uncovering the covert networks employed by state actors across the competition continuum, including Chinese and/or Russian use of deniable assets, proxies, and covertly funded, supported, or enabled nonstate actors. China and Russia work to keep their covert, hybrid activities cloaked or, at the very least, screened by misinformation; if revealed, they assess their networks will become fragile or ineffective or otherwise become a liability.

The toolkit developed to illuminate nonstate threat networks thus represents a potentially powerful means to push back against China and Russia across the competition continuum. For example, further exposing the web of Chinese and Russian complicity with North Korea's sanctions evasion (by identifying specific ships involved, their links back to Chinese or Russian firms, and the exact location of illicit transfers) provides U.S. decisionmakers with expanded options to increase pressure on them to fully enforce UN sanctions.

Uncovering the connections with proxies can also provide U.S. decisionmakers with options to counter this type of activity. The Chinese or Russian government entities involved with nonstate proxies can be identified by a demarche and/or targeted by sanctions. If the United States chooses to go public with information on the extent of Russian or Chinese state involvement, this could have a chilling effect on the proxy's future ability to conduct its operations; once the association is public, China or Russia may cease its support to the now-exposed proxy, thus degrading its malign activity. In other cases, this threat illumination can uncover how these states employ parastate actors for the purposes of espionage or even kinetic action abroad and in turn allow the United States and its allies response options such as demarches or other types of disruptive actions against Beijing or Moscow.

In addition, projects to secure land and maritime boundaries against illicit WMD smuggling networks provide U.S. partners and allies with critical capabilities to identify and interdict proliferation of WMD-related materials, dual-use items, and delivery systems tied to Russia or China. Disrupting these networks can help prevent proliferation of these materials to nonstate actors seeking WMD capabilities.

These efforts to prevent proliferation of WMD and related materials across land borders also build broader partner nation border security capabilities that can be applied to U.S. and allied efforts to stymie certain Chinese and Russian activities below the level of armed conflict. Moscow has breached land boundaries to move forces, seize strategic territory, undermine institutions, and conduct covert attacks (including with WMD), while China repeatedly interferes with maritime boundaries in its efforts to bully its neighbors into accepting its control over the Western Pacific. DTRA's efforts to help Jordan better detect and interdict WMD and related materials at its borders and to help the Southeast Asian nations detect and interdict WMD trafficking in their maritime domains are also relevant to countering revisionist power efforts to

Bahrain Defense Force servicemember showcases protective chemical and biological protective suit to exercise participants of United Arab Emirates Union Defense Force, at Al Wathba, UAE training facility, as part of exercise Leading Edge, January 28, 2013 (U.S. Marine Corps/Leon M. Branchaud)

infiltrate and interfere with the sovereign space of U.S. allies and partners.

The United States has a range of options to counter Russia and China across the competition continuum, including tools and approaches honed during the battle against VEOs. Now that the United States recognizes the challenge posed by Moscow and Beijing within this space, it is important that we adapt to meet the strategic environment in which we now operate.

Potential Risks

In doing so, however, it is also critical to proceed carefully, deliberately, and, wherever possible, in tandem with allies and partners. State and nonstate threat networks share a number of features and operating procedures, but the risks in countering state networks are significantly higher and must be factored into the calculus of U.S. decisionmakers. When engaging with nonstate threat networks in the past, the United States could act without the risk of initiating a strategic conflict that posed an existential threat to the country. In the future, the United States will need to carefully consider whether to target a key node of a state network—such as a foreign military intelligence official funneling weapons to a nonstate proxy—if undertaking such an action could prompt a retaliatory attack on U.S. forces. Moreover, in addition to the immediate costs incurred, this response by a revisionist power could potentially escalate to a state-on-state armed conflict.

Another risk is that many revisionist power malign activities involve (sometimes witting, sometimes unwitting) third-party actors. The potential consequences of alienating third parties must also be taken into account, particularly as long-term success in countering Russia and China will require deepened cooperation with current and new U.S. partners or allies.

Conclusion

Russia and China use a wide range of unconventional methods to achieve their objectives of undermining international order and fracturing U.S.-led regional security architectures. Thanks to robust U.S. nuclear and conventional capabilities, these state actors remain deeply wary of the risks of direct armed conflict with the United States and its allies and partners. This has pushed their competition with the United States below the threshold of state-on-state armed conflict that is neither a stable peace nor a hot war.

The United States has demonstrated the capability to operate across the conflict continuum, though we must take steps to adapt our operations to this new strategic environment and increase the capacity to conduct such actions on a larger scale to counter revisionist and rogue states' global threat networks. Tools and approaches developed to reveal and dismantle nonstate threat networks have considerable value in countering the malign activities of state adversaries and their agents and proxies. As the United States gears up for the challenge posed by revisionist powers, DTRA stands ready to support U.S., allied, and partner efforts to illuminate adversary threat networks and enable action to exploit, disrupt, and defeat these networks and their operations. JFQ

Notes

[1] Kristina Hummel, "A View from the CT Foxhole: Vayl S. Oxford, Director, Defense Threat Reduction Agency," *CTC Sentinel* 12, no. 3 (March 2019), 11, available at <https://ctc.usma.edu/view-ct-foxhole-vayl-s-oxford-director-defense-threat-reduction-agency/>.

[2] *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense [DOD], 2018), 2.

[3] "Statement of Vayl Oxford," House Armed Services Committee, Subcommittee on Intelligence and Emerging Threats and Capabilities, April 3, 2019, available at <https://armedservices.house.gov/?a=Files.Serve&File_id=C5D34C82-5AE0-4753-B798-47C9DE77919E>. The phrase *improvised threats* refers to improvised explosive devices (IEDs), unmanned aerial systems, and other threats to U.S., allied, and partner forces that are sourced, developed, assembled, and employed outside of the processes associated with the more formal, structured, and deliberate development of weapons associated with weapons fielded by state armed forces.

[4] Joint Doctrine Note 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), v, available at <www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.

[5] Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (1st Quarter 2016), 102, available at <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/>.

[6] "Top NATO Commander Concerned About 'Little Green Men' in Moldova," Reuters, September 17, 2014, available at <www.atlanticcouncil.org/blogs/natosource/top-nato-commander-concerned-about-little-green-men-in-moldova>.

[7] Robert R. Leonhard, Stephen P. Phillips, and Johns Hopkins University Applied Physics Laboratory Assessing Revolutionary and Insurgent Strategies (ARIS) Team, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014* (Fort Bragg, NC: U.S. Army Special Operations Command, July 2016), available at <www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf>.

[8] Gregory B. Poling, "Illuminating the South China Seas Dark Fishing Fleets," Center for Strategic and International Studies, January 9, 2019, available at <https://ocean.csis.org/spotlights/illuminating-the-south-china-seas-dark-fishing-fleets/>.

[9] "Imposition of Chemical and Biological Weapons Control and Warfare Elimination Act Sanctions on Russia," press statement, Department of State, August 8, 2018, available at <www.state.gov/imposition-of-chemical-and-biological-weapons-control-and-warfare-elimination-act-sanctions-on-russia/>.

[10] "Novichok Nerve Agent Use in Salisbury: UK Government Response, March to April 2018," Government of the United Kingdom, April 18, 2018, available at <www.gov.uk/government/news/novichok-nerve-agent-use-in-salisbury-uk-government-response>.

[11] Their joint efforts, however, failed to carry votes on investigations into the use of chemical weapons in the Salisbury case or regarding the conflict in Syria; unlike the United Nations (UN) Security Council, the major powers do not have special veto powers separating them from other state parties to the Chemical Weapons Convention.

[12] Sergei Khazov-Cassia and Robert Coalson, "Russian Mercenaries: Vagner Commanders Describe Life Within the 'Meat Grinder,'" Radio Free Europe/Radio Liberty, March 14, 2018, available at <www.rferl.org/a/russian-mercenaries-vagner-commanders-syria/29100402.html>.

[13] *2017 Report on Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments* (Washington, DC: Department of State, 2017), available at <www.state.gov/2017-report-on-adherence-to-and-compliance-with-arms-control-nonproliferation-and-disarmament-agreements-and-commitments/#Missile4>.

[14] Fatima Bhojani, "How ISIS Makes IEDs: The Supply Chain of Terrorism," *Foreign Affairs*, March 2, 2016, available at <www.foreignaffairs.com/articles/2016-03-02/how-isis-makes-ieds>.

[15] "Statement by Ambassador Haley on Reports of Russian Violations of UN Security Council Resolutions," U.S. Mission to the United Nations, August 3, 2018, available at <https://usun.usmission.gov/statement-by-ambassador-haley-on-reports-of-russian-violations-of-un-security-council-resolutions/>; "U.S. Accuses Russia of Altering UN Report on North Korea Sanctions," Radio Free Europe/Radio Liberty, September 14, 2018, available at <www.rferl.org/a/u-s-accuses-russia-of-altering-un-report-on-north-korea-sanctions/29489277.html>.

[16] Lolita C. Baldor, "U.S. Defense Chief Sends Message to China with Photos Showing North Korea Sanctions Go Unenforced," Associated Press, June 11, 2019, available at <www.militarytimes.com/news/pentagon-congress/2019/06/11/acting-us-defense-chief-shared-photos-with-chinese-counterpart-that-show-north-korea-sanctions-go-unenforced/>.

[17] "Japan Says Fighter Jets Scramble after Russian Military Aircraft Violate Airspace," Radio Free Europe/Radio Liberty, June 21, 2019, available at <www.rferl.org/a/japan-says-fighter-jets-scramble-after-russian-military-aircraft-violate-airspace/30011921.html>; "Statement by General Terrence J. O'Shaughnessy," Senate Armed Services Committee (SASC), February 26, 2019, available at <www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-26-19.pdf>.

[18] SASC, "Statement by General Terrence J. O'Shaughnessy."

[19] Joint Publication 3-25, *Countering Threat Networks* (Washington, DC: The Joint Staff, December 21, 2016), viii, available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_25.pdf>.

[20] David Richard Doran, "Outmatched: Shortfalls in Countering Threat Networks," *Joint Force Quarterly* 89 (2nd Quarter 2018), 28, available at <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1491501/outmatched-shortfalls-in-countering-threat-networks/>.

[21] "Department of Defense Press Briefing by Admiral Kurt Tidd," video, 31:01, U.S. Southern Command, March 6, 2018, available at <www.southcom.mil/Media/Speeches-Transcripts/Article/1458781/department-of-defense-press-briefing-by-admiral-kurt-tidd/>.

[22] Doran, "Outmatched," 30.

[23] Clay Wilson, *Improvised Explosive Devices (IEDs) in Iraq: Effects and Countermeasures*, RS22330 (Washington, DC: Congressional Research Service, February 10, 2006), available at <www.hsdl.org/?view&did=715089>.

[24] "U.S. Security Cooperation with Jordan," fact sheet, Department of State, May 21, 2019, available at <www.state.gov/u-s-security-cooperation-with-jordan/>.

Pararescueman with 82nd Expeditionary Rescue Squadron, deployed in support of Combined Joint Task Force–Horn of Africa, participates in static line jump from 75th Expeditionary Airlift Squadron C-130J Hercules near Camp Lemonnier, Djibouti, May 11, 2019 (U.S. Air Force/Chris Hibben)

Development Beyond the Joint Qualification System

An Overview

By Dina Eliezer, Theresa K. Mitchell, and Allison Abbe

In 1986, Congress passed the Goldwater-Nichols Department of Defense Reorganization Act, leading to substantial reforms in joint officer personnel policy and management.

Dr. Dina Eliezer is a Research Staff Member at the Institute for Defense Analyses (IDA). Theresa Mitchell, JD, is a Research Staff Member at IDA. Dr. Allison Abbe is a Professor of Organizational Studies at the U.S. Army War College.

Goldwater-Nichols requirements were based on concerns that the Department of Defense (DOD) had paid insufficient attention to joint officer management and on a perception that there were disincentives to serving in joint assignments. Twenty years after Goldwater-Nichols, continued congressional interest in joint officer development resulted in the 2007 requirement for DOD to establish different levels of joint qualification and supporting criteria for each level.[1] In response to this congressional requirement, DOD evaluated the state of Joint Officer Management (JOM) and the Joint Specialty Officer designation process and implemented the Joint Qualification System (JQS) to support a more strategic human resource approach to JOM.[2]

The JQS is a system of progressive career development steps intended to prepare officers for unified action at the operational and strategic levels. Under the current JQS, officers become credentialed as Joint Qualified Officers through a combination of education and experience, and this designation is required for promotion to general officer/flag officer. The experience requirement can be met either through standard joint duty assignments (S-JDA) after service in a Joint Duty Assignment List (JDAL) position or through joint experience points obtained from experience in non-JDAL joint duty assignments and experiences that demonstrate an officer's mastery of knowledge, skills, and abilities in joint matters (experience-based joint duty assignments, or E-JDA). For both S-JDA and E-JDA, the preponderance of duties must involve joint matters as defined by statute.

The JQS recognizes that significant experience in joint matters is gained through operations supported by joint task forces and other organizations, such as the interagency community and international and nongovernmental partners, as well as through joint exercises and joint training events or courses. At the time of its implementation, the definition of *joint matters* was fairly general and focused on the joint aspects of military operations: "matters related to unified action by multiple military forces in operations across domains such as land, sea, or air, in space, or in information environment."[3] As a result, the JQS was originally intended to include a broad range of experiences, including joint training, education, participation in exercises, and self-development learning opportunities, as well as non-JDAL joint assignments.

Subsequent changes to the definition of joint matters and associated policy since 2007 have limited credit for E-JDA and S-JDA to strategic roles and select education and assignment opportunities. Changes to the definition in 2016 shifted the focus to the strategic mission level: "the development or achievement of strategic objectives through synchronization, coordination, and organization of integrated forces in operations conducted across domains, such as land, sea, or air, in space, or in the information environment."[4] Additionally, other changes to the JOM policy have limited what are considered joint experiences. For instance, experiences in which the officer is not responsible for implementation of joint policy or program—for example, as a student or in a fellowship or in assignments affiliated with a degree-granting institution or research program—are not eligible for consideration.

Joint Leader Competencies

By focusing solely on the strategic level, the JQS omits a host of joint experiences that may nonetheless be important for building joint competencies. Despite changes to JOM policy and a narrowing of the joint matters definition since 2007, successful leadership in joint environments continues to require a broad set of competencies. In a study on developing Army officers for the joint environment, the officers interviewed cited the importance of joint knowledge, including awareness of the function, capabilities, and cultures of other governments, agencies, or Services.[5] They also emphasized the importance of critical thinking and expertise in their functional specialties. However, above all else, officers emphasized the importance of interpersonal skills, explaining that in joint environments it is essential to develop relationships, listen to diverse viewpoints, and motivate disparate groups to collaborate toward a common goal. Another study of senior executive service members, Reserve component and general and flag officers, and noncommissioned officers arrived at similar conclusions about the skills needed in joint environments. Interviewees emphasized the importance of general people and leadership skills, understanding of other organizations, knowledge of joint operations and doctrine, and expertise in their own fields.[6]

Despite an adequate understanding of the skills needed in joint environments, officers are not always sufficiently prepared for assignments at joint commands. In one study of Joint Staff officers and their senior leaders serving in assignments at the nine combatant command headquarters, more than half of respondents indicated that the learning curve required in their position was 7 months or longer.[7] This amounted to almost one-third of a 22- to 24-month assignment period. Part of the skill deficit may be due to a lack of education, as about three quarters of Joint Staff officers had not yet attended joint professional military education Phase II courses. Furthermore, given that nearly half of the headquarters billets were at the O-4 level and below, officers may have lacked a sufficient career history of joint duty assignments, deployments, and exercises to prepare them for the position.

To better prepare personnel for these roles, the Services and Joint Staff should consider developmental assignments more systematically and promote joint development at an earlier career stage. Formal joint professional military education specifies learning outcomes, instructional methods, and content, and aligns assessments to those learning outcomes. Informal experiential learning, by definition, does not lend itself to the same degree of structure; nonetheless, experiential learning through assignments can be part of a developmental career progression that sets the conditions for systematically building joint competencies over time.

Challenging Experiences Build Competency

Joint development is best completed through a progressive model or building-block approach whereby leaders are exposed to a wide range of increasingly complex and challenging learning experiences. These opportunities to progressively develop the joint competencies described above are not limited to just the strategic level or to formal educational settings, as predicated in the current JQS. Rather, research suggests that a broad range of experiences builds competency, particularly in areas of knowledge that lack clear guidelines or specific sets of rules.[8] Knowledge that is acquired through experience and that cannot be articulated through a formalized set of rules is referred to as *tacit knowledge*. In this context, tacit knowledge includes understanding

Patrolman with 22nd Security Forces, McConnell Air Force Base, Kansas, receives some motivational words from Phoenix Raven instructor during intensive 3-week, 12-hour-a-day Phoenix Raven Qualification Course at Joint Base McGuire-Dix-Lakehurst, New Jersey (U.S. Air Force/Vernon Young, Jr.)

how to work with and lead others of different backgrounds, shape the environment, and contribute and combine Service-specific resources in the joint environment. This learning through application or experience-based tacit knowledge is especially important for problem-solving and has been linked to favorable performance among military and business leaders.[9] Tacit knowledge may be particularly important for joint assignments, given the scope of responsibilities and the competencies required.

Foundationally, experiences must be sufficiently challenging, complex, and broad to have a significant impact on leadership development. Developmentally enhancing experiences often involve high levels of responsibility while performing novel tasks, implementing change, working across functional domains, and working with diverse groups.[10] These challenging experiences promote joint development because they push individuals to think beyond parochial Service perspectives, expend greater effort, cope with uncertainty, reflect on their outcomes, and develop new behaviors.[11] A wealth of empirical research supports the positive relationship between challenging work environments and development. In fact, supervisors rate junior managers as more competent when they are positioned in challenging assignments.[12] Leaders indicate that they developed the most in positions that were different from their typical assignments.[13]

While it is important to provide challenging and diverse developmental experiences, individuals also vary in their abilities to draw the appropriate lessons from these challenging experiences and then generalize those lessons to subsequent experiences. Leaders early in their careers are more apt to develop and modify their behaviors in response to challenging experiences, compared to more experienced leaders. Experienced leaders may have well-established belief systems and patterns of behavior that are less amenable to change when compared to their younger counterparts. Less-experienced leaders simply have more to learn and may be more willing to adapt and change.[14]

Implications for Joint Leader Development

As reflected in the research above, to develop joint competency in the military, it is necessary to place Servicemembers in *challenging* joint environments early in their careers. Joint environments require leaders to manage a complex set of individual and group relationships, all while executing a technically challenging and novel mission. Not all joint experiences may be sufficient to develop joint competency. To contribute significantly to development, experiences must be novel, complex, and difficult, without creating overwhelming cognitive demands.[15] This points to a progression of multiple, increasingly challenging joint experiences over one's career.

To assess whether the types of experiences recognized in the JQS meet these criteria, we reviewed a subset of E-JDA self-nominations, limiting the review to Air Force submissions that were disapproved in calendar year 2017. E-JDA submissions are reviewed by JQS Experience Review Panels three times per year. Panels determine whether each submission meets the joint matters criteria, does not meet the criteria, or should be rewritten. The panels then make a recommendation to the Vice Director of the Joint Staff.

When considering whether to award joint credit for an experience, the JQS Experience Review Panels assess both the "how" (the nature of the work completed) and the "who" (with whom the officer worked). Guidance to the panels requires that joint experiences must be strategic in nature and meet the other elements of the joint matters definition—for example, involving interaction with personnel from another Service, with other U.S. departments or agencies, with foreign military or agencies, or with nongovernmental entities. Although the who component of this requirement is quite broad, the strategic focus limits the scope of experiences eligible for joint credit.

The review of Air Force E-JDA submission denials confirmed the limitations of the system described herein. Although the E-JDA submission form requests information on what members did and with whom they did it, the decisions recommended by the panels do not appear to reflect consideration of the who, but instead rely almost exclusively on the what. Most of the disapproved submissions reported experiences involving supervisors and peers from other Services, foreign militaries, and U.S. agencies or non-DOD entities, but they did not receive joint credit due to the tactical or operational level of the work. Thus, the JQS recognizes joint experiences at only one mission level rather than encouraging a progression of experiences that develops leaders over time. Strategically focused joint experiences are certainly critical, but experiences at the tactical and operational levels are important components of a developmental progression toward joint and strategic leadership. The extent to which an experience is broadening and challenging likely plays more of a role in determining joint development than the specific mission level.

By focusing solely on the strategic level, the JQS omits a host of joint experiences that are important for the Services to encourage, track, and assess for their own joint leader development efforts. Additionally, current Service career milestones may not incentivize joint experiences at early career stages. This limited scope may be necessary from a DOD perspective; providing too many officers with joint qualification through E-JDA may deplete the supply of officers available for JDAL positions. However, from a Service perspective, the limited scope of the JQS provides no benefit and could serve as a disincentive for personnel to seek a variety of challenging joint experiences. Because officers early in their careers likely have the most to gain from the challenge of a joint experience, it is advisable to encourage joint experiences through alternative mechanisms outside the JQS. The Services often retain their best talent for Service leadership positions at the expense of exposing members to a greater breadth of joint experiences at different levels.

Broader approaches to assess, track, and manage joint capabilities are needed within the Services to develop a fully joint-competent force. Service-specific approaches to recognize a wide range of joint experiences throughout the career cycle should emphasize the value of joint matters, encourage Servicemembers to pursue joint opportunities, and support more informed personnel management. It is important for the Services and DOD to recognize and convey the value of joint experiences for career development. Joint experiences are broadening experiences; they provide opportunities to develop general leadership and problem-solving skills that can be applied to both Service-specific and joint domains.

The Air Force Joint Talent Tracking and Management Initiative

Airmen bring unique Service perspectives and capabilities to the complex challenges of joint warfighting. Yet the Air Force is underrepresented in the senior joint positions most influential for national security strategy and warfighting, as well as Joint Staff positions that are seen as preparatory positions for senior levels of joint command. Various factors may explain this underrepresentation, but one important reason may be that the Air Force often develops its top talent for positions within the Service rather than for joint leadership.[16] Moreover, as revealed in the review of the 2016 Air Force E-JDA submissions, Airmen are gaining valuable joint experiences that are not recognized under the JQS, which can serve as a disincentive to seeking joint experiences that would help develop joint leaders.

Recognizing the need for greater emphasis on joint development within the Air Force, the Chief of Staff of the Air Force, General David L. Goldfein, established "Strengthening Joint Leaders and Teams" as an Air Force key focus area to advance the Air Force's Future Operating Concept, Strategic Master Plan, and Air Force priorities. In response, the Air Force initiated 26 supporting projects to improve joint development. One of these projects is the Joint Talent Tracking and Management (JTTM) initiative to assess, track, and manage joint experience within the Air Force.

The JTTM initiative recognizes the need to value and track both traditional and nontraditional joint experiences across different career fields. The current joint matters definition in the JQS is too narrowly focused on strategic roles and has been limited to joint officer development, whereas the Air Force aims to track and encourage a broad range of joint experiences for all Airmen (officers, enlisted, and civilians). Accordingly, the Air

Explosive ordnance disposal technicians assigned to 466th Air Expeditionary Squadron walk toward blast pit after detonating four 500-pound bombs during demolition day, March 16, 2014 (U.S. Air Force/Vernon Young, Jr.)

Force broadened the definition of what is considered joint.

Specifically, JTTM uses a broad Air Force–specific definition of *joint experiences*: "an assignment or experience that develops or demonstrates mastery of knowledge, skills, and abilities in joint, interagency, intergovernmental, or multinational (JIIM) topics or activities." JIIM experiences include not only billets and operational assignments, but also education, exercises, and other experiences. The definition aligns with joint policy, adapting the definition of E-JDA in the Chairman of the Joint Chiefs of Staff Instruction on JOM, but expands the range of experiences and extends beyond officers to enlisted Airmen and civilians. Additionally, the JTTM development team defined a set of indicators to use in identifying, validating, and potentially valuing these experiences. The indicators, drawn from previous studies regarding joint experience, are as follows: type of experience, duration of the experience, exposure to non–Air Force personnel or organizations, organizational level, mission level, joint functions, and joint role.[17]

To ensure that Airmen had a voice in the initiative, the JTTM development team gathered input from Career Field Managers and other Airmen when developing the definition and indicators. Career Field Managers tested a precoding questionnaire to assess officer and enlisted assignments on the joint experience indicators (duration, exposure to non–Air Force personnel or organizations, organizational level, mission level, joint functions, and joint role). Additionally, both officer and enlisted Airmen completed self-nomination questionnaires describing their joint assignments, deployments, and education along the indicator dimensions. The study initially involved career fields that were known to have joint experiences, such as air liaison, explosive ordnance disposal, medical corps, judge advocate general corps, logistics, and weather, but later extended to a broader range of fields (for example, foreign area officers, cyber, intelligence, force support, mobility pilots, fighter pilots, and airfield operations).

Responses to the precoding and self-nomination questionnaire indicated a diverse range of joint experiences, roles, and functions available to Airmen. Most respondents indicated that exposure to JIIM personnel or organizations occurred on a daily or weekly basis. The majority of precoded questionnaires identified experiences at the tactical level, while about half of self-nominated questionnaires were at the operational level. Given that the majority of these experiences lacked a strategic focus, they would not be eligible for E-JDA credit, yet they clearly demonstrated exposure to a broad range of joint experiences in a variety of domains.

In a related initiative, the Air Force is working to refine joint knowledge standards as part of its Institutional Competencies. Many of these joint competencies align with the knowledge, skills, and abilities described by officers and other senior leaders in the research highlighted above, particularly those pertaining to joint knowledge. Recognizing the interdependency between joint competency and leadership competency in general, the joint competencies were developed to align with the Air Force's broader competency framework. This allows for a greater integration of joint skills throughout career development.

Currently, the Air Force is working to implement its Institutional Competencies (including joint competencies), JTTM, and other joint development initiatives. Next steps for JTTM include developing the processes and information technology to support the collection and storage of JIIM experience information for use in career development. In combination with the other joint development initiatives, the Air Force's JTTM system will directly promote joint career development by conveying the value the Air Force places on joint experiences, encouraging more Airmen to pursue joint opportunities, and supporting more informed personnel management. Broadening the tracking of joint experiences beyond officers and to a wider spectrum of experiences, including tactical and operational joint exposure, will enable the Air Force to develop a deeper pool of joint competent and credible Airmen across all ranks. The Air Force's enhancement of its tracking and management of joint experiences for all Airmen acknowledges the crucial role of enlisted and civilian Airmen and the fact that officers serve as only one element of the Air Force team in a joint fight.

Conclusions

Joint experiences provide the kinds of complex "stretch" assignments that contribute to leadership development. A variety of joint experiences at all mission levels (for example, tactical, operational, and strategic) can place Servicemembers in complex situations, expose them to diverse perspectives, and require them to engage in new behaviors and ways of thinking that develop stronger leaders. As such, joint experiences should be considered as valuable for their potential to develop not only joint competencies but also broader leadership and problem-solving skills that will transfer to both joint and senior Service leadership. The Services should plan for these experiential assignments more deliberately, developing the bench for future joint leadership earlier in members' careers.

Today's adversaries are increasingly challenging the United States by employing lethal and nonlethal effects across multiple domains and regions. As military operations grow in sophistication and complexity, the value of joint leaders who have progressed through developmentally challenging joint experiences will increase. The JQS focus on officers working at the strategic level will be insufficient to build the joint-ready force needed to meet our nation's warfighting demands. It is time to move beyond a strategic and officer-centric joint development focus and ensure that joint development encompasses the total force. Joint officers cannot succeed without civilian and enlisted leaders who are similarly developed for joint roles. The Air Force has taken steps to enhance joint development that can serve as a model for the other Services in developing their own career development processes to better prepare leaders for the demands of joint operations. These efforts should proceed in close coordination with the Joint Staff, consistent with JOM and education policies, to ensure that career development meets both Service and joint requirements. **JFQ**

Notes

[1] H.R. 5122, Pub. L. 109-364, *John Warner National Defense Authorization Act of Fiscal Year 2007.*

[2] Government Accountability Office (GAO), *Joint Officer Development Has Improved, but a Strategic Approach Is Needed*, GAO-03-238 (Washington, DC: GAO, 2002); *Independent Study of Joint Officer Management and Joint Professional Military Education* (Washington, DC: Booz Allen Hamilton, 2003); and Harry J. Thie et al., *Framing a Strategic Approach for Joint Officer Management* (Santa Monica, CA: RAND, 2005); Chairman of the Joint Chiefs of Staff Instruction 1330.05A, *Joint Officer Management Program Procedures* (Washington, DC: The Joint Staff, December 15, 2005).

[3] "Department of Defense Joint Officer Management Joint Qualification System Implementation Plan," March 30, 2007, A-4.

[4] Title 10, U.S. Code, § 668, *National Defense Authorization Act for Fiscal Year 2017.*

[5] M. Wade Markel et al., *Developing U.S. Army Officers' Capabilities for Joint, Interagency, Intergovernmental, and Multinational Environments* (Santa Monica, CA: RAND, 2011).

[6] Raymond E. Conley et al., *Enhancing the Performance of Senior Department of Defense Civilian Executives, Reserve Component General/Flag Officers, and Senior Noncommissioned Officers in Joint Matters* (Santa Monica, CA: RAND, 2008).

[7] *The Joint Staff Officer Project, Final Report* (Washington, DC: The Joint Staff, April 2008).

[8] Morgan W. McCall, Jr., "Developing Executives Through Work Experiences," in *Human Resource Planning: Solutions to Key Business Issues*, ed. David M. Schweiger and Klaus Papenfuss (Wiesbaden: Gabler Verlag, 1992), 219–229; and Cynthia D. McCauley, *Leader Development: A Review of Research* (Greensboro, NC: Center for Creative Leadership, 2008).

[9] Jennifer Hedlund et al., "Identifying and Assessing Tacit Knowledge: Understanding the Practical Intelligence of Military Leaders," *The Leadership Quarterly* 14, no. 2 (2003), 117–140; and Robert J. Sternberg and Richard K. Wagner, "Tacit Knowledge: An Unspoken Key to Managerial Success," *Creativity and Innovation Management* 1, no. 1 (1992), 5–13.

[10] Cynthia D. McCauley, Patricia J. Ohlott, and Marian N. Ruderman, *Job Challenge Profile, Facilitator's Guide: Learning from Work Experience* (San Francisco: Jossey-Bass/Pfeiffer, 1999); Cynthia D. McCauley et al., "Assessing the Developmental Components of Managerial Jobs," *Journal of Applied Psychology* 79, no. 4 (1994), 544; and Patricia J. Ohlott, "Job Assignments," in *The Center for Creative Leadership Handbook of Leadership Development*, ed. Cynthia D. McCauley and Ellen Van Velsor (San Francisco: Jossey-Bass, 2004), 151–182.

[11] D. Scott DeRue and Ned Wellman, "Developing Leaders via Experience: The Role of Developmental Challenge, Learning Orientation, and Feedback Availability," *Journal of Applied Psychology* 94, no. 4 (2009), 859.

[12] Lisa Dragoni et al., "Understanding Managerial Development: Integrating Developmental Assignments, Learning Orientation, and Access to Developmental Opportunities in Predicting Managerial Competencies," *The Academy of Management Journal* 52, no. 4 (August 2009), 731–743.

[13] Morgan W. McCall, Jr., and George P. Hollenbeck, *Developing Global Executives: The Lessons of International Experience* (Cambridge: Harvard Business School Press, 2002).

[14] Giles Hirst et al., "Learning to Lead: The Development and Testing of a Model of Leadership Learning," *The Leadership Quarterly* 15, no. 3 (2004), 311–327.

[15] DeRue and Wellman, "Developing Leaders via Experience," 859.

[16] Caitlin Lee et al., *Rare Birds: Understanding and Addressing Air Force Underrepresentation in Senior Joint Positions in the Post–Goldwater-Nichols Era* (Santa Monica, CA: RAND, 2017).

[17] John F. Schank et al., *Who Is Joint? Reevaluating the Joint Duty Assignment List* (Santa Monica, CA: RAND, 1996); Sheila Nataraj Kirby et al., *Who Is "Joint"? New Evidence from the 2005 Joint Officer Management Census Survey* (Santa Monica, CA: RAND, 2006); and Margaret C. Harrell et al., *A Strategic Approach to Joint Officer Management: Analysis and Modeling Results* (Santa Monica, CA: RAND, 2009).

Titanium parts printed from powder and laser provide researchers with high-strength, heat-resistant examples of future of additive manufacturing (U.S. Army/David McNally)

3D Printing for Joint Agile Operations

By Jaren K. Price, Miranda C. La Bash, and Bart Land

The Navy seabase off the coast of Africa is like a floating hive, with personnel moving about aboard multiple ships and both aircraft and landing craft launching to deliver the second wave of the assault force to their objectives. Teams of mechanics examine several Army and Marine Corps vehicles recovered from the beach via landing craft air cushion. One team triages damage in preparation for repairs required for expedited return of the vehicles to the field. Another team assesses the more significant damage done to a joint light tactical vehicle (JLTV) that struck a mine. The mechanics submit requests for repair parts. Some parts are immediately retrieved from stores located on the seabase, while manufacturing specialists load blueprints from a database for those parts not already on hand. Soon, three-dimensional (3D) printers hum. Meanwhile, the specialist engineering team develops a repair solution for the JLTV, and an engineer drafts the 3D design. The new plans are also transferred to print production. The parts are delivered to the mechanics who then complete the repairs. Within hours, the vehicles are ready for return to their units.

In the near future, this scenario could become reality. Additive manufacturing (AM), also known as 3D printing, could enable future agile operating concepts. AM has the ability to significantly shorten the Department of Defense (DOD) logistics chain, especially where repair parts are concerned, by producing the parts as they are needed. This would enable rapid, flexible response to unanticipated faults or battle damage with reduced stockpile requirements, increasing the agility of the operational force. However, to

Colonel Jaren K. Price, USA, is the Deputy Commander of the U.S. Indo-Pacific Command Joint Intelligence Operations Center. Lieutenant Commander Miranda C. La Bash, USN, serves in the Intelligence Directorate at U.S. Special Operations Pacific Command. Major Bart Land, USAF, is the North East Asia Logistic Planner in the Directorate of Logistics, Engineering, and Security Cooperation at U.S. Indo-Pacific Command.

fully and efficiently capitalize on the potential of AM, DOD must develop common data solutions and standardized safety, certification, and requisition processes for AM, leveraging data science to prioritize development efforts by cost savings and implementation impact. An integrated effort by the joint enterprise is required to overcome Service independence and technology implementation challenges to make joint agile sustainment a reality.

The December 2017 National Security Strategy identifies Russia and China as revisionist powers that are actively competing with the United States across all domains.[1] They have developed weapons to asymmetrically exploit U.S. weaknesses and create standoff through antiaccess/area-denial and area-denial strategies. Outside the realm of nation-state competition, the United States continues to carry out humanitarian and antiterrorism operations in austere environments. These developments mandate that the United States devise the means to operate in contested environments and in places where access to bases and infrastructure does not readily support operations.[2] A key aspect of future operations is how to effectively sustain the joint force.

Based on this vision for the future, the Services have laid out concepts and started to develop capabilities and procedures for agile operations in an array of denied environments. The new operating concepts envision sustained ground, naval, and tactical air operations being conducted without access to ports, airports, or staging bases for extended periods and operating from austere airfields with only the minimum logistics support. These tactics require logisticians to develop new ways to meet the needs of the force, providing timely sustainment without the use of large land-based logistics facilities. These concepts include the Navy and Marine Corps' Seabasing Concept, a variety of Air Force Disbursed/Agile Basing Options, and the Army's Multidomain Operations.

Whether operating from floating seabases, dispersed airfields, or remote operating bases, these concepts call for U.S. forces to be able to maneuver from strategic distances and integrate capabilities across time and space to overmatch the enemy. Implementing these concepts requires "precision logistics that provides a reliable, agile, and responsive sustainment capability."[3] The enemy is expected to specifically target U.S. sustainment capabilities both at home and at deployed locations by conventional, unconventional, and cyber means. Thus, sustainment forces must often be dispersed to multiple locations, be resilient to attack, and have enough redundancy to maintain baseline capability in spite of attacks on some locations. They also call for sustaining, maintaining, and repairing units and equipment as far forward as possible.

The common theme among all the operating concepts is the ability to deliver sustainment support as far forward as possible, reduce the requirement for large logistic bases, and protect the joint force through minimizing its size and operational footprint. While equipment and spare parts make up only a small fraction of sustainment requirements compared with fuel and ammunition, AM at forward locations would help realize these concepts by reducing required spares inventory, shrinking lift requirements, creating more flexible prepositioned stocks, and providing redundancy.

The term *AM* appropriately describes a process that involves adding and bonding consecutive layers of material, whereas traditional (subtractive) manufacturing involves shaping and milling and usually secondary materials specifically engineered for the creation of one design (such as a mold). The removal of material during traditional manufacturing results in a much larger percentage of waste of the base material than AM does. AM generates the capability to rapidly manufacture spare parts in the local vicinity, eliminating supply chain distances and often prolonged acquisition processes. It has fixed per unit costs, enabling the efficient production of small quantities of custom parts. Besides the ability to recreate previously out-of-production parts, AM facilitates unit-level innovations such as the production of custom tools to solve niche problems.[4] Other potential benefits of AM for manufacturing include networked smart factories, improved quality control, rapid innovation, individualization with voxel-by-voxel[5] digital modifications, and on-demand production, reducing inventories.[6] Incorporating AM into the manufacturing process can also reduce part count, assembly time, and weight "while creating complex internal and external geometries that could not be made any other way."[7]

At a distance from both repair facilities and spare parts storage, units employing agile operating concepts could manufacture their own replacements or leverage a nearby forward base, significantly reducing stocked inventory, transport requirements, and time to get needed parts to repair facilities. To maintain operations in denied areas, avoid detection, reduce equipment downtime, and maximize repair opportunities while under way or in the field, units with AM capabilities could create parts on demand.

Currently, each Service has its own system of mobile warehouses that contain replacement parts for specific weapons systems such as fighter aircraft. Mobile warehouses enable our current expeditionary capabilities but require significant enhancement in order to support agile operating concepts. These mobile warehouses rely on extensive amounts of demand data to forecast with modest accuracy what should be maintained in stock. Demand data can be best described as the frequency with which certain items are required. Collected over years, this data forms a picture of the replacement parts required over time for each system on record.

Demand data, however, cannot predict all critical failures, leaving weapons systems susceptible to mission degradation for prolonged periods of time. New systems have no demand data, making predictive schedules for replacement parts difficult. Legacy weapons systems have failures that were never anticipated, meaning no replacement parts were ever produced. They may also have components that are no longer manufactured. AM has the potential to reduce risk associated with unanticipated demand by

Army researcher Dr. Brandon McWilliams holds sample part created from powder at U.S. Army Combat Capabilities Development Command's Army Research Laboratory, Aberdeen Proving Ground, Maryland, February 25, 2019 (U.S. Army/David McNally)

enabling production at the point of need. In addition, AM enables leaner mobile warehouses because the risk generated by out-of-stock parts is reduced or eliminated through on-site manufacturing.

The technology does not yet allow for the elimination of these mobile warehouses, but it will allow stocks focused on low-density, high-demand parts, particularly complex parts or parts requiring materials or precision not easily produced under current AM capabilities. More effective and condensed mobile warehouses and global stocks will lighten the burden on transportation assets and the distribution system. On a large scale, this would result in reduced personnel and materiel-handling equipment at distribution hubs, en route locations, and agile bases. Some of these personnel could instead be trained to become AM specialists. With fewer aircraft, ships, trucks, and rail cars required to move items through the supply chain, these transportation assets could instead concentrate on the delivery of operational forces and equipment to and from agile bases.

Transportation assets, such as cargo aircraft and ships, would also benefit from an onboard or isolated location AM capability to support organic repair capabilities. Units could make their own critical parts on-site, allowing distribution missions to continue on schedule. This would be especially useful when transportation assets do not include mobile warehouse capabilities or are themselves long distances from logistics support. The increased availability of transportation assets created by this capability would allow resources to be committed to other operational needs. It would also enable more frequent trips to isolated agile bases without increased investment in transportation assets.

Adding an AM capability to prepositioned stocks would directly support agile basing concepts. The Army, Marines, and Air Force depend on these ships to be ready to respond to crises, but there are only a few ships maintained worldwide due to the immense investment required to operate each. These stocks consist of a large variety of items that enable crucial weapons systems and combat personnel including, but not limited to, materiel-handling equipment, construction equipment, generators, radios, refueling equipment, medical equipment, and ammunition. AM could be utilized to allow more robust maintenance and repair actions on board for both the ship and stock, averting frequent returns to port to restock. Returning to port takes days to weeks and often includes significant homeport maintenance periods, reducing platform availability for crisis action and increasing risk to potential operations. AM would provide a means to mitigate this risk.

Another advantage of utilizing AM is the avoidance of sunk costs due to obsolescence or end of service life. As military equipment is modernized over time, prepositioned stock must be updated, incurring periodic reinvestment costs. Some of this replacement stock is also discarded due to expiring shelf life despite having never been used. AM helps reduce these costs by enabling production of equipment when it is actually needed. When AM technology matures, the increased equipment produced at the time of need may allow for the conversion from a few large prepositioned stock vessels to a larger number of small but equally capable ships. This will be possible because AM will be able to produce complex pieces of equipment custom made for the mission. These ships could more effectively provide coverage for global operations, creating a much more responsive prepositioned stock. Improving the prepositioned stock fleet in this way is critical to making agile operating concepts a reality.

Units across DOD are already beginning to innovate utilizing AM to develop new tools and to streamline maintenance and supply procedures. The Marine Corps Iwakuni Engine Ship Kit, created by a technician in the unit using a 3D printer, allows for the movement of aircraft engines requiring repair without draining oil and hydraulics.[8] Marine Corps Systems Command and Marine Corps Installations and Logistics have created a transportable 3D print lab prototype, X-FAB (Expeditionary Fabrication Lab), for use with deployed maintenance forces. The Chief of Naval Operations' Rapid Innovation Cell has permanently installed one printer on the USS *Essex*[9] and has plans to install 3D printers on two additional ships.[10] Naval Sea Systems Command (NAVSEA) has also approved the first metal part created by AM for a 1-year trial on the USS *Harry S. Truman*.[11]

To support forward-deployed Soldiers, U.S. Army Research, Development, and Engineering Command (RDECOM) has partnered with the Rapid Equipping Force to help manage, staff, and support its own 3D printing Expeditionary Labs (Ex Labs), which can be deployed worldwide. The Army Ex Lab is a fabrication laboratory, self-contained in a 20-foot shipping container. It contains four 3D printers, currently limited to polymer printing.[12] One is deployed to Bagram Airfield in Afghanistan, and another is operating out of Camp Arifjan, Kuwait.[13] This enables solutions to problems discovered on the battlefield, but current policy strictly confines AM to only emergency repairs. Furthermore, to produce a repair part, Soldiers are required to simultaneously requisition the item through the supply system.[14]

The Defense Department has already made significant investments in AM technology, and America Makes—the National Additive Manufacturing Innovation Institute—was established in 2012 as a public-private partnership between the Federal Government, private industry, and universities. It is managed by the Air Force Research Laboratory (AFRL).[15] As a significant marker of progress in the partnership, in June 2018, America Makes and the American National Standards Institute published version 2.0 of the AM Standardization Roadmap, highlighting the gaps in and steps to standardize the lifecycle of an AM part.[16] This work will go a long way to boost industry development of AM that can eventually be used by DOD.

Meanwhile, disparate organizations within the Services are pursuing database design and parts validation for AM. The Navy has designated OPNAV N4 as lead Navy synchronizer for AM.[17] RDECOM and U.S. Army Materiel Command are creating a product data management system to retain and share design data.[18] RDECOM, the Office of Naval Research, and AFRL all have laboratories that conduct AM research activities.[19]

The U.S. Government Accountability Office recommended in October 2015 that DOD designate an Office of the Secretary of Defense (OSD) lead for the development and implementation of a systematic approach to Department-wide activities and resources that facilitate the adoption of AM technology across DOD. The primary driver is an ability to track actual or potential performance and combat capability improvements, cost savings, and lessons learned.[20] Over a year later, on November 30, 2016, a joint committee composed of Service, Defense Logistics Agency (DLA), and America Makes leads published a DOD AM Roadmap containing high-level goals for continued development and implementation of AM objectives. The committee assessed significant coordination across the Services but suggested that more formal sharing mechanisms and progress assessments were required, including the assignment of a lead integrator to coordinate DOD AM Roadmap revisions.[21] Despite coordination, it is unclear if an OSD lead was ever named, and each of the Services has developed or is developing its own AM roadmap and independent capabilities.

In order to enable AM for maintenance and logistics, the whole of AM implementation across DOD must be matured. The independently produced AM implementation plans for the Army, Navy, and Air Force take separate approaches to developing AM across the force. Only with unity of effort can DOD efficiently overcome nine key implementation challenges:

- material standards and availability
- part selection
- skill set development
- configuration control
- reproducibility
- cyber security
- part validation and qualification
- process validation and qualification
- ability to reverse-engineer components.[22]

And these challenges must be overcome in order to achieve AM capabilities that can support agile operating concepts. For shorter term limited employment of AM for repair parts, most critical is the ability to develop, share, and retain Technical Data Packages (TDPs), which make parts printable, and the ability to reproducibly print to adequate precision and quality in the design-specified materials. To enable AM for part production more generally, a prerequisite for reliable, competitive sourcing of spare parts is a mature industry of AM manufacturers using comparable printers, with a defined set of material standards and file formats.[23]

The engineering and post-processing intensity required for most parts means that printing qualified parts will be difficult to achieve in austere environments. A part must be qualified, or certified, to meet certain design specifications (temperature, pressure, forces, and motion over certain amount of time), in order to be installed in a DOD system. For a 3D part to be qualified, it must be printed from a qualified printer: an AM printer that has been itself certified as able to reproduce the part to the same specifications with each use. Competitive bidding is also required among potential manufacturers, translating into a requirement to certify multiple models of printer (in use at different companies or built by different manufacturers) that would need to be qualified for each part.

Materials must also be certified by a defined standard, increasing the developmental work required by DOD to leverage a still immature field to this task. In alloy production, there are currently only a few metals with an American Society for Testing Materials standard defined for AM. And for metal AM techniques, significant facility and operational requirements exist to accurately and consistently create parts, including controlled temperature, humidity, movement, and reliable electrical power, containment of powders to prevent accidental transport and contamination of alloys on hand, specialized equipment to clean the machine, and material that must be disposed of—the creation of soot-laden waste water in the machine itself.[24] To date, these constraints have restricted field printing to polymers.

The variety of raw materials required to manufacture repair parts is another limitation that will need to be considered. Systems design engineers will need to find ways to reduce the diversity of materials in order to permit leaner AM material stocks. For example, it may be advantageous to use more expensive materials for some parts that do not actually require them in order to use a single material across several components, simply to reduce AM raw material variety required in stock. To implement AM in support of mobile warehouses, the right balance between stocking replacement parts and raw materials is also required to maximize the effectiveness and minimize the overall size of all stock.

In order to most effectively develop AM to support agile logistics, several things must occur. First, a secure unified digital network across DOD, containing certified TDPs themselves as well as metadata regarding the printer, supplier data, and certifying engineering activity, is required. DLA Logistics Operations Research and Development is developing such a database in coordination with the Services. It is also developing a repeatable supplier qualification process and has developed a limited Additive Part Candidate Identification Tool to help identify which parts to prioritize for production using AM.[25] For the development of new systems, contract language to handle intellectual property issues and enable future access to precise technical data will be key to successfully harness AM capabilities in the long term.

Second, DOD must develop standardized processes across the Services. NAVSEA, the Naval Warfare Centers, and DLA are building standardized processes and guidelines for AM and developing TDPs for parts that can no longer be acquired through normal supply channels. The Naval Warfare Centers, Systems Centers, and Naval Research Laboratory are studying how best to qualify and certify 3D printed parts. Naval Surface Warfare Center Port Hueneme is also looking at applications on ships, specifically on the logistics, data libraries, contracting mechanisms, and issues regarding data rights.[26] Process validation remains rather intensive, with three different printers at three different locations test printing a single TDP in order for DLA to then put out a bid for the contract manufacture of that part. One Warfare Center materials engineer, however, has suggested that eliminating the requirement to qualify every individual part is required to realize AM's true potential.[27] Because it is not cost effective to validate in this way every part that a unit might want to print or design, there should be a streamlined process for those parts meeting a lower threshold of system criticality. Whatever the standard, there must be a single standard implemented across DOD.

Third is shifting the requisition process to incorporate AM, leveraging a centrally managed database of qualified parts to print where they are needed instead of requisitioning parts through normal supply channels. Robust multifunction printing would then be viable at in-theater depots. Although the Services would largely print different parts, there is likely to be some overlap in parts and significant overlap in qualified printers and materials, making unified and compatible systems by design as well as federated testing absolute must-haves for efficiency.

Fourth, safety standards must be published and implemented. This includes safety considerations for closed spaces, such as shipboard environments or conex boxes. The AM work environment must both contain materials and allow adequate ventilation in order to prevent hazards to personnel, such as toxic gases released during fusion of metal powders.[28] The use of personal protective gear and adequate detection of and ventilation for a possible gas leak from within a metal printer's inert gas atmosphere are required. This capacity must be integrated within safety procedures and hazardous waste programs.

Depending on part complexity, material, and the AM capabilities forward, some parts offer greater differential advantage to stock rather than print. An important fifth step in implementation is prioritizing which parts should be developed for AM. Paired to part prioritization is developing the level of printer capabilities that would be most useful forward. Costs and capabilities vary widely for 3D printers, pricing anywhere from $2,000 for a home plastics printer to $50,000 for a basic metal printer to over a million dollars for a larger, more accurate multi-material printer. Differentiating both parts and printers across a range of attributes, including size, material, and resolution requirements, is critical to establishing which parts can realistically be fabricated locally and which would be better produced in more specialized facilities, whether land-based, in-theater, or back with the manufacturer. Some parts, critical but difficult to precisely print, would need to be retained in stock. For mission-critical parts that can be precisely

Marines with 7th Engineer Support Battalion and Sailors with Naval Mobile Construction Battalion 5 attach hose onto 3D concrete printer during 3D Concrete Printing exercise at Camp Pendleton, California, December 9, 2018 (U.S. Marine Corps/Betzabeth Y. Galvan)

3D printed—such as engine components—whether steam plant or aviation, weapons systems, and safety systems, a long lead of material, printer, and part qualification is required to ensure the parts meet specifications.

Sixth, DOD must broadly assess which spare parts across the inventory would offer economic and operational advantage if shifted to AM. This would enable the prioritization of over 5 million line items across the Defense Department for further investigation, with unity of effort and potential federation across Service channels.[29] Applying data scientists to this effort will help systems engineers prioritize their efforts. Criteria for AM at point of need should include high or intermittent demand, long lag to receipt at supply depot, criticality of readiness impact without component, printing capability to produce a qualified part if required, and accessibility of design specifications in a TDP repository. Adaptive modeling and visualization of which policy adaptations, joint collaboration opportunities, and technical solutions are most useful for increasing capabilities forward, while reducing cost would advise the most beneficial focuses over time across the DOD enterprise.

Finally, it is critical that the most cost-effective methods and processes be determined. The cost calculations for an AM implementation must include the total cost of facilities, training or contracting of operators, unified databases with mechanisms to allow for intellectual property rights of the designs, ongoing fabrication materials costs, software and machine service contracts, and program management over time.[30] As AM is developed, the cost savings that can be realized across DOD if the Services appropriately leverage economies of scale and avoid duplicative efforts cannot be overemphasized. While relatively segregated today across Services, TDP development, database creation and maintenance, contracting methods, safety standards, and AM policy can and must be accomplished jointly.

AM implementation across the Department of Defense is in its early stages. Current experimentation with AM across the Services demonstrates applications for agile operations, emergency situations, and innovative uses. However, there are significant program development hurdles ahead to reach AM's potential. The DOD must identify cross-Service solutions that will generate a distinct operational advantage when factors such as repair time and cost are considered. Some of the most immediate challenges include developing databases of parts that can be printed locally; establishing DOD-wide methods and requirements for safety, parts, and printer certification; and determining which parts are best printed locally and which should

Prototype parts are 3D-printed in new Advanced and Additive Manufacturing Center of Excellence to troubleshoot machines at Joint Manufacturing and Technology Center, Rock Island Arsenal, Illinois, May 15, 2019 (U.S. Army/Debralee Best)

be stocked or supplied through more traditional supply channels. AM is a key enabler for joint agile sustainment, but joint must be part of the design.

The world is changing rapidly, and potential adversaries will aim to rob the United States of all of her advantages. As we envision fighting in austere locations and areas where we are denied access to robust logistics bases, AM, if properly developed, represents a potential advantage for U.S. forces. JFQ

Notes

[1] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 25, available at <www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

[2] U.S. Army Training and Doctrine Command Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations, 2028* (Washington, DC: Headquarters Department of the Army, 2018), iii, available at <www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf>.

[3] Ibid.

[4] Lance M. Bacon, "Here's How Marines Are Using 3-D Printing to Make Their Own Parts," *Marine Corps Times*, April 30, 2016, available at <www.marinecorpstimes.com/news/your-marine-corps/2016/04/30/here-s-how-marines-are-using-3-d-printing-to-make-their-own-parts/>.

[5] *Voxel*, a combination of the words *volume* and *pixel*, describes the smallest modifiable volume of a 3D-printed object.

[6] Luiz Durão et al., "Additive Manufacturing Scenarios for Distributed Production of Spare Parts," *International Journal of Advanced Manufacturing Technology* 93, nos. 1–4 (2017), 869–880.

[7] Paul Sharke, "How Practical Is 3-D Metal Printing?" *Mechanical Engineering* 139, no. 10 (2017), 44–49.

[8] Bacon, "Here's How Marines Are Using 3-D Printing to Make Their Own Parts."

[9] Daniel Kent and Michael Carvelli, "Looking at 3-D Printing from All Sides Now: New Technology Offers Major Benefits for Army Maintenance," *Army Magazine*, November 2016, 19–21.

[10] Government Accountability Office (GAO), *Defense Additive Manufacturing: DOD Needs to Systematically Track Department-Wide 3D Printing Efforts*, GAO 16-56 (Washington, DC: GAO, 2015), 1–44, available at <www.gao.gov/assets/680/673099.pdf>.

[11] "NAVSEA Approves First Metal Additively Manufactured Component for Ship," NAVSEA News, October 11, 2018, available at <www.navsea.navy.mil/Media/News/Article/1659370/navsea-approves-first-metal-additively-manufactured-component-for-shipboard-use/>.

[12] Steve Stark, "Why the Hype? Additive Manufacturing Is All the Rage, but Why?" *Army AL&T Magazine*, January 28, 2019, 91–95.

[13] Argie Sarantinos-Perrin, "A New Dimension of Acquisition," *Army AL&T Magazine*, November 28, 2016, 82–87.

[14] Steve Stark, "Complex Geometry: Additive Manufacturing Holds Great Potential, but Much Work Remains to Be Done for the Army to Get to Additive Nirvana," *Army AL&T Magazine*, January 23, 2019, 75–83.

[15] GAO, *Defense Additive Manufacturing*.

[16] American National Standards Institute

(ANSI), "America Makes and ANSI Publish Version 2.0 of Standardization Roadmap for Additive Manufacturing," *ANSI.org*, June 28, 2018, available at <www.ansi.org/news_publications/news_story?menuid=7&articleid=fc19f3c2-de56-4d96-9d42-cc0c7a0c8c37>.

[17] Jason T. Ray, "Additive Manufacturing in the Navy: State of the Technology," *Navy Supply Corps Newsletter*, June 2, 2016, available at <http://scnewsltr.dodlive.mil/2016/06/02/additive-manufacturing-in-the-navy-state-of-the-technology/>.

[18] Sarantinos-Perrin, "A New Dimension of Acquisition."

[19] GAO, *Defense Additive Manufacturing*.

[20] Ibid.

[21] Jennifer Fielding et al., *Department of Defense Additive Manufacturing Roadmap*, Report 88ABW-2016-5841 (Washington, DC: Department of Defense, November 30, 2016), 1–34, available at <www.americamakes.us/wp-content/uploads/sites/2/2017/05/Final-Report-DoDRoadmapping-FINAL120216.pdf>.

[22] Amanda M. Schrand, "Additive Manufacturing in the DOD," *DSIAC Journal* 5, no. 4 (Fall 2018), available at <www.dsiac.org/resources/journals/dsiac/fall-2018-volume-5-number-4/additive-manufacturing-dod>.

[23] Bill Decker, "Harnessing the Potential of Additive Manufacturing," *Defense AT&L*, November–December 2016, 31–34, available at <www.dau.mil/library/defense-atl/DATLFiles/Nov-Dec2016/Decker.pdf>.

[24] "7 Steps to Prepare Your Shop for Metal Additive Manufacturing," Modern Applications News, available at <www.modernapplicationsnews.com/cms/man/opens/article-view-man.php?nid=2&bid=741&et=featurearticle&pn=10>.

[25] Kelly Morris, "Driving Innovation to Support the Warfighter," *Defense AT&L*, November–December 2016, 43–47, available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/1029460.pdf>.

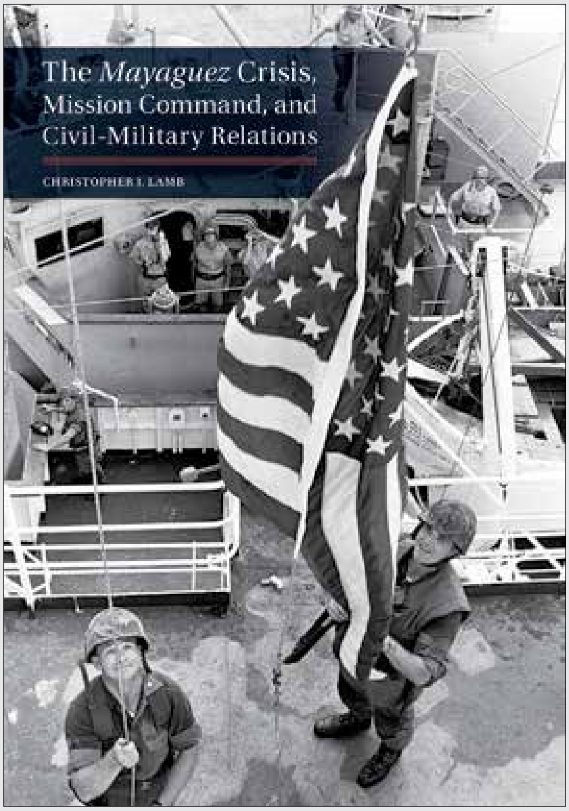
[26] Edward Lundquist, "As 3D Printing Evolves, So Do Emergency Repairs," *Naval Forces* 38, no. 2 (March 2017), 65–67.

[27] Ibid.

[28] "7 Steps to Prepare Your Shop for Metal Additive Manufacturing."

[29] Michael Kidd, Angela Quinn, and Andres Munera, "Additive Manufacturing: Shaping the Sustainment Battlespace," *Joint Force Quarterly* 91 (4th Quarter 2018), 40–46, available at <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1681686/additive-manufacturing-shaping-the-sustainment-battlespace/>.

[30] Mike Vasquez, "Embracing 3D Printing," *Mechanical Engineering* 137, no. 8 (August 2015), 42–45.



New from the Office of Joint History

The Mayaguez Crisis, Mission Command, and Civil-Military Relations

By Christopher J. Lamb
2018 • xxiv + 284 pp.

President Gerald R. Ford's 1975 decision to use force after the Cambodians seized the USS *Mayaguez* merchant ship is one of the best documented but least understood crises in U.S. history. U.S. behavior is still explained as a rescue mission, a defense of freedom of the seas, an exercise in realpolitik, a political gambit to enhance Ford's domestic political fortunes, and a national spasm of violence from frustration over losing Vietnam. Widespread confusion about what happened and why it did contributes to equally confused explanations for U.S. behavior.

Now, with new sources and penetrating analysis, Christopher J. Lamb's *The Mayaguez Crisis, Mission Command, and Civil-Military Relations* demonstrates how three decades of scholarship mischaracterized U.S. motives and why the common allegation of civilian micromanagement during the crisis is wrong. He then extracts lessons for current issues such as mission command philosophy, civil-military relations, and national security reform. In closing he makes the argument that the incredible sacrifices made by U.S. Servicemen during the crisis might have been avoided but were not in vain.

Women's Auxiliary Air Force radar operator Denise Miley plotting aircraft on cathode ray tube of RF7 receiver in Receiver Room at Bawdsey Chain Home radar station (Courtesy Royal Air Force, Imperial War Museum, Goodchild)

The Chain Home Early Warning Radar System
A Case Study in Defense Innovation

By Justin Roger Lynch

The Germans were aimed to facilitate an amphibious landing across the Channel, to invade this country, and so to finish the war. . . . Mine was the purely defensive role of trying to stop the possibility of an invasion, and thus give this country a breathing spell. . . . I had to do that by denying them control of the air.

—Air Chief Marshal Hugh Dowding

The United Kingdom began the Battle of Britain in an unenviable position. After the fall of France and evacuation of Dunkirk, Britons were justifiably concerned about Germany's next move and the potential for an attack on England. Fortunately, when the Luftwaffe attack came, the British government had already created the world's first integrated air defense system.

The Chain Home early warning radar system played an important role in Great Britain's defense during the Battle of Britain. The system's ability to warn the Royal Air Force (RAF) about incoming Luftwaffe attacks helped restore a measure of Britain's isolation from continental states, contributing to the resistance to and eventual defeat of Nazi Germany. Much of the story of the Chain Home system is already known. Today, however, its creation serves as a case study in military innovation; it shows the importance of allowing strategy to inform the acquisition process, adapting rapidly during war, and having the right team to manage development and implementation.

Context

British scientists created the Chain Home system during a time when the relative strength of the offense and defense was shifting. During World War I, trench warfare challenged the logistics of the day, hindering the exploitation of tactical victories and therefore preventing armies from achieving decisive results for the majority of the war.[1] During the interwar period, some theorists believed the creation of powerful bomber aircraft would allow air forces to bypass enemy armies and geographical boundaries, shifting the balance back toward the offense.[2]

Airpower's growing offensive capabilities changed Britain's strategic outlook. During previous conflicts, the British relied on the English Channel and the Royal Navy to prevent powerful continental armies from invading. The combination of the two formed a barrier that had remained intact for centuries.[3] British fleets protected England from attack by the Spanish Armada in 1588, by Napoleon at Trafalgar in 1805, and by German land forces during World War I. Airpower threatened to allow rivals to bypass the Channel and the fleet, negating Britain's traditional defense. Adversaries possessing powerful air forces would be able to directly target the British population, industry, and infrastructure. In some ways, this returned the British to a vulnerability they had not experienced since medieval times.

At the same time, Nazi Germany's increasingly aggressive rhetoric and powerful air force convinced Britons they needed to develop a defense against their most likely threat.[4] The Luftwaffe had demonstrated its potential during the Spanish Civil War by bombing Guernica.[5] A war between Germany and Britain promised to see similar actions. By the late 1930s, the Germans planned an invasion of England that relied heavily on using the Luftwaffe to strip British defenses and to destroy the population's morale via terror bombing.[6] As a result, the British began to develop a system to defend themselves against aircraft in the same manner the Channel and Royal Navy had defended against ground and naval forces.[7]

The Creation of Chain Home

The British government began to dedicate significant resources to the development of radar in January 1935. The government asked Robert Watson-Watt, a scientist at the National Physical Laboratory, about the feasibility of creating a radio death ray. In February, his team conducted the Daventry experiment. They mounted a short-wave British Broadcasting Company transmitter and a receiver onto commercial vans, then transmitted radio waves along the flight path of a bomber to see if aircraft would deflect radio waves.[8] He reported that while death rays were unlikely to succeed, radio waves could detect aircraft.[9] By June, he demonstrated bistatic continuous wave (CW) radar, which separates transmitters and receivers in order to generate interference when an object flies between the two. While an advance, bistatic CW radar was too limited for practical use. In September, Watson-Watt's team demonstrated the pulse radar detection the Chain Home system would eventually use.[10] One of the government officials who received Watson-Watt's report reacted by proclaiming, "Once again Britain is an island."[11]

The government approved construction of a coastal radar system while research was still ongoing. It authorized the system in September 1935, the same month Watson-Watt tested pulse radar detection. In December, it approved the expenditure of £60,000 to build 5 stations.[12] Each transmitting station consisted of a pair of 100-meter-tall steel towers with 2 dipole arrays hanging on wires between them. The receiving stations were east-west and north-south running dipole antennas mounted on approximately 245-foot-tall wooden towers.[13]

After proving the concept, the British government began construction of a complete system. Coastal radar systems went into continuous service in the spring of 1938. By September 1939, the government had installed 20 stations along the majority of Britain's east coast, establishing the Chain Home system.[14] For approximately £10 million, Britain created a system that detected aircraft out to 120 miles, providing roughly 20 minutes warning, from technology that did not exist at the beginning of the acquisition process.[15]

Early versions of the Chain Home system had two major problems. The first was its inability to detect low-flying aircraft. The original system detected aircraft between 25,000 and 1,000 feet above ground level, creating the potential for German aircraft to evade detection. To resolve this issue, the RAF added Chain

Justin Roger Lynch served as an Active-duty Army officer before transferring to the Army National Guard. As a civilian, he has served in multiple roles in the national security enterprise, including roles focused on emerging technology.

Home Low, a series of shorter portable towers that could detect aircraft flying at 500 feet.[16] The second problem was the skill needed to interpret radar signals. Early displays used oscilloscopes that required complex calculations to determine target locations.[17] The creation of the Plan Position Indicator, which showed the target's position on a map displayed on a cathode ray tube, resolved the issue by reducing the number of calculations needed and making the display more instinctive.[18]

The Chain Home system quickly became an important part of Great Britain's defense. With the system in place, the British received a warning. German aircraft staged for their attacks by gathering in France in full view of the Chain Home system.[19] Combined with information from Ultra and the Observer Corps, Chain Home gave the RAF time to intercept the Luftwaffe before it could bomb RAF bases or civilian populations, allowing the British to save their resources for an eventual counterattack.[20] While they were far from completely safe, they could use their isolation to protect their strategic base from the German army and, as necessary, use their island as a staging area for forces to fight on the continent, as they had in World War I and the Napoleonic Wars.

Lessons for Military Innovation

One of the most important lessons from the development of Chain Home is the need for strategy to inform operational needs and therefore the acquisition process. The interwar period was a time both of dramatically changing military technology and miniscule defense budgets. The RAF was primarily focused on creating a strategic bomber force. Many of its leaders were convinced that bombers would always be able to make it through air defense systems and that strategic bombing could independently win wars. As a result, other parts of the air force, such as Fighter Command, were usually neglected during budgetary decisions.[21]

Rather than dedicating their limited resources toward the latest new technology or trying to match their potential adversaries, the RAF and British political leaders decided they needed to defend the Home Islands from the type of air attacks they experienced in 1917 and 1918.[22] Their determination led to an investment in Fighter Command, which, with support from its political allies, decided that it needed advance notice of air forces coming from the continent to prevent adversaries from gaining control of the air—thus the need for Chain Home.[23]

Chain Home's development also testifies to the importance of rapid innovation in war. The system was a direct response to the advent of effective bomber aircraft, strategic bombing concepts, and Adolf Hitler's aggressive rhetoric. The system subsequently transitioned from a theoretical concept in January 1935 to an operational coastal defense system in September 1939.[24] Walter Kaiser claims, "It is probable that never before or since has such a major technical advance been so widely and successfully deployed in such a short time."[25] If the British government had been slower to act in recognizing its problem set, initiating research, or implementing construction, the system might not have been ready before the Battle of Britain. Even if Chain Home had not existed, the Luftwaffe might not have been able to destroy either Britain's will or capacity to fight. It is likely, however, that without a warning of incoming German aircraft, more RAF fighters would have been destroyed on their runways, and the Luftwaffe would have dropped more bombs on British cities.

It is also unlikely that Chain Home would have been ready if the RAF had not used an iterative development process. Developers using iterative processes make incremental changes to their product rather than try to create a perfect solution from the start. Each iteration is an opportunity to learn rather than a verdict on the system's potential. This allows for less-than-perfect advancements that are still improvements and for regular real-world tests throughout the development process rather than waiting until the end to test the whole system.

An iterative development process can create useful systems more quickly than one that seeks perfection from the start. The Chain Home team developed the program incrementally, developing and implementing flawed systems as long as they were an improvement to the current system and there was a reasonable probability the flaws could be fixed. Watson-Watt tested his theory using existing technology designed for different purposes.[26] Six months later, he had developed a prototype and received the funding needed to create a working system.[27] The first system's inability to detect low-flying aircraft or function without significant mathematical expertise by the user also did not halt its production. Instead, the government accepted that it would need to continue iterating the system's design. The willingness to accept an imperfect design in order to generate progress allowed the government to continue advancing the project and create the Chain Home system before the Battle of Britain.

A third lesson from the development of Chain Home and its integration with Fighter Command is the importance of having the right team in place to foster the growth of specific innovations. It can be tempting for innovative thinkers to believe their idea's or program's merits should stand on their own. This is, somewhat unfortunately, not true. Great ideas and programs rarely survive the uphill climb against bureaucratic inertia based solely on their merits. Programs also need leaders that can shepherd them through the existing system. The expertise to do so, and the bureaucratic, diplomatic, and emotional intelligence it requires, is just as important to program implementation as tactical and technical expertise. In this case, Chain Home had a military champion, entrepreneur, and technical expert.[28]

Hugh Dowding served as the military champion. He advocated for radar within the military bureaucracy, ensured that military personnel partnered with engineers to make sure they both understood operational needs and how the system could perform, and helped develop the tactics the RAF could use to capitalize on Chain Home's capabilities, particularly for night airborne interceptions.

Watson-Watt was the group's entrepreneur. He negotiated with government organizations and industry groups, suggested the line of stations that eventually became Chain Home, and helped acquire the funding streams to turn the group's ideas into reality. Sir Henry Tizard was the technical expert. His committee helped anticipate the system's potential capabilities and issues, including the limitations of air interception, how to communicate air warnings, information quality control, and how to guide aircraft to their targets. Without all three performing their roles, it would have been far more difficult to identify radar's potential, acquire the funding needed to develop it, and integrate it into Fighter Command.

Team composition may differ based on the technology being developed and the system being worked through, but every team needs technical, military, and bureaucratic expertise. Without a technical expert, teams struggle to understand the nuances of development, purchasing, creating requirements, and maintaining new capabilities. This can result in unrealistic expectations, new technology that does not actually perform the task it was designed for, and long-term maintenance problems.

Military experts serve several roles. They help ensure technology will be effective by identifying operational needs, potential friction points during real-world use, and how a particular capability will fit in with the rest of the military. Military experts connect their team to the operational force, easing implementation. They also help add legitimacy so that the acquisition system will take the program seriously.

Bureaucratic experts are necessary because development and acquisition take place in a vast, confusing space filled with red tape. However, they are also filled with opportunities for those who understand the system to make a meaningful difference. A team member who understands the Federal Acquisition Regulation, Other Transaction Authorities, and a host of other regulations, processes, and personalities allows a team to move through the acquisition process and focus on shipping the product instead of fighting a bureaucracy.

Lessons about effective development and acquisition are incredibly relevant for the joint force. The 2018 National Defense Strategy notes that "our competitive military advantage has been eroding" in an environment defined by rapid technological changes and other factors.[29] The ability to identify actual and potential strategic threats, define capability deficits, and create solutions will be an important part of retaining an advantage.

Today's defense development and acquisition systems can learn from the history of the development of the Chain Home early warning radar system. While the above lessons are helpful, perhaps the most important lesson is the focus and willingness to take risks shown by Dowding, Watson-Watt, Tizard, and their teams. Radar systems did not exist in 1935 when the government agreed to fund one. They based their path ahead on the sense of urgency created by their strategic environment, a prototype, and the belief they could iterate their way to a successful system. Without a similar attitude, any group of innovators is less likely to succeed. **JFQ**

Notes

[1] John Keegan, *The First World War* (New York: Vintage Books, 2000), 174–182.

[2] Giulio Douhet, "The Command of the Air," in *Roots of Strategy: Book 4*, ed. Curtis Brown (Mechanicsburg, PA: Stackpole Books, 1987), 283.

[3] Alfred Gollin, "England Is No Longer an Island: The Phantom Airship Scare of 1909," *Albion* 13, no. 1 (1981), 43.

[4] R.J. James, "A History of Radar," *IEE Review* 35, no. 9 (1989), 344.

[5] Russell A. Hart, *Clash of Arms: How the Allies Won in Normandy* (Boulder, CO: Lynne Rienner, 2001), 50.

[6] William L. Shirer, *The Rise and Fall of the Third Reich: A History of Nazi Germany* (New York: Simon & Schuster, 1960), 760.

[7] Walter Kaiser, "A Case Study in the Relationship of History of Technology and of General History: British Radar Technology and Neville Chamberlain's Appeasement Policy," *Icon* 2 (1996), 32.

[8] James, "A History of Radar," 344.

[9] Kaiser, "A Case Study in the Relationship of History of Technology and of General History," 35.

[10] Merrill I. Skolnik, "Fifty Years of Radar," *Proceedings of the IEEE* 73, no. 2 (1985), 182.

[11] James, "A History of Radar," 344.

[12] Otto Kreisher, "Radar from World War II Until Today," *Naval Forces* 3 (2007), 71–72.

[13] Ibid.

[14] Skolnik, "Fifty Years of Radar," 38.

[15] Kaiser, "A Case Study in the Relationship of History of Technology and of General History," 37.

[16] Ibid., 38.

[17] Kreisher, "Radar from World War II Until Today," 70–71.

[18] Kaiser, "A Case Study in the Relationship of History of Technology and of General History," 39.

[19] Kreisher, "Radar from World War II Until Today," 71.

[20] Joseph F. McCloskey, "British Operational Research in World War II," *Operations Research* 35, no. 3 (1987), 454.

[21] Hart, *Clash of Arms*, 37–38.

[22] Williamson Murray, *Military Adaptation in War: With Fear of Change* (Cambridge: Cambridge University Press, 2011), 156–158.

[23] Colin Gray, "Dowding and the British Strategy of Air Defense 1936–1940," in *Successful Strategies Triumphing in War and Peace from Antiquity to the Present*, ed. Williamson Murray and Richard Sinnreich (Cambridge: Cambridge University Press, 2014), 241.

[24] Skolnik, "Fifty Years of Radar," 38.

[25] Kaiser, "A Case Study in the Relationship of History of Technology and of General History," 41.

[26] James, "A History of Radar," 344.

[27] Skolnik, "Fifty Years of Radar," 182.

[28] Alan Beyerchen, "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom, and the United States," in *Military Innovation in the Interwar Period*, ed. Williamson Murray and Allan R. Millett (Cambridge: Cambridge University Press, 1998), 282–283.

[29] *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), 3.

Death of General Wolfe, by Benjamin West, 1770, oil on canvas, National Gallery of Canada (Courtesy of The Yorck Project)

Wolfe, Montcalm, and the Principles of Joint Operations in the Quebec Campaign of 1759

By Joseph Finnan, Lee P. Gray, John H. Perry, and Brian Lust

A critical campaign analysis of the French and Indian War's 1759 Quebec campaign demonstrates that Britain achieved victory because it reflected the principles of joint operations better than its French enemy did. While the British lacked a doctrinal publication that listed principles of joint operations, the thought processes and underlying concepts similar to our current doctrinal principles unmistakably shaped their military thought.

British General James Wolfe achieved decisive victory at Quebec because he creatively integrated many of these principles in his operational plan, thereby magnifying their effect. Committing to a clear strategic objective while practicing

Dr. Joseph Finnan is an Intelligence Officer in the Defense Technology and Long-Range Analysis Office at the Defense Intelligence Agency. Major Lee P. Gray, USA, is a Political-Military Officer at Headquarters, U.S. Africa Command. Lieutenant Commander John H. Perry, USN, is on the Joint Staff J5. Lieutenant Colonel Brian Lust, USA, is a Joint Transportation Planner at U.S. Transportation Command.

effective unity of command between the army and navy allowed Wolfe to practice economy of force with the troops he had available. He retained the operational offensive, exploiting masterful amphibious maneuver and achieving dramatic surprise in order to deploy overwhelming mass at the decisive point of the campaign. Conversely, his opponent, General Marquis de Montcalm, displayed isolated adherence to some of these principles, but his failure to integrate them into an overall approach limited their impact and led to defeat.

Quebec Campaign of 1759

After achieving naval superiority in North America and conquering the French Atlantic fortress of Louisbourg in 1758, British war plans targeted Quebec City, the capital of New France, as the primary objective for 1759. Consequently, Wolfe led his British expedition of 9,000 men up the St. Lawrence River, landing initially on Ile d'Orléans, downriver from Quebec, on June 26, 1759. Wolfe sought to draw his opponent, Montcalm, out from his defensive positions where he could conduct a decisive engagement. Montcalm refused to oblige. Wolfe ordered an artillery barrage of Quebec in early July, staged a frontal assault at Montmorency on July 31, and conducted an operation in August of widespread destruction throughout the French-Canadian countryside. With winter quickly approaching, Wolfe faced the loss of his supporting naval squadron. He opted for a bold offensive move to draw Montcalm out of his tactical defense. He therefore staged a daring nighttime amphibious operation on September 13, where 4,000 British regulars sailed downriver to a cove called the Anse au Foulon, climbed the bluff there, and moved onto the Plains of Abraham west of the city. Montcalm, unprepared for the British move, decided to attack the British line with a combination of roughly 4,500 French regulars, Canadian militia, and Native allies. Concentrated musket fire from the British regulars broke the French advance and cost France the battle. An additional force of French regulars led by the Comte de Bougainville arrived after the climactic effort, but quickly withdrew. Both Wolfe and Montcalm suffered mortal wounds in the engagement, and the remaining French garrison inside Quebec surrendered on September 17, 1759, resulting in a decisive British campaign victory.[1]

Wolfe and the Traditional "Principles of War"

Wolfe's experience suggests that joint officers should take it upon themselves to analyze historical case studies and not leave such examination solely to formal military instruction. Joint officers need to tie the lessons of abstract principles to historical examples, as well as connect them to their own personal experiences, in order to internalize and apply these principles in complex and unanticipated future environments.

While today's designation of 12 "principles of joint operations" is anachronistic for the 18th century, Wolfe largely taught himself the military arts and acquired a familiarity with the traditional principles of war. He read military theory and history widely, including writers from antiquity such as Thucydides, Julius Caesar, and Xenophon, as well as more recent military thinkers like Gustavus Adolphus, Charles XII of Sweden, and Vauban. Wolfe lamented Britain's lack of formal military education and argued that "our military education is by far the worst in Europe. We are the most egregious blunderers in war." Wolfe strongly favored critical analysis of past campaigns "to exercise the faculty of judging," making the practical case that "the more a soldier thinks of the false steps of those that are gone before, the more likely he is to avoid them."[2]

Wolfe also fortified his appreciation for these principles through firsthand military experience, an option also available to today's joint officers. Wolfe identified his preoccupation with the principle of mass after his experience at the battle of Dettingen, in Germany in 1743, where as a junior officer he fruitlessly went on "begging and ordering the men not to fire at too great a distance, but to keep it till the enemy should come near us; but to little purpose." As a commander, he rigorously trained his troops in musket fire: "firing balls at objects teaches the soldier to level incomparably, makes the recruits steady, and removes the foolish apprehension that seizes young soldiers." Similarly, he honed his appreciation for the principles of maneuver and surprise during the abortive British amphibious effort against Rochefort on the French coast in 1757. Wolfe deduced important lessons for amphibious actions: "lose no time in getting troops on shore. . . . generals should settle their plan of operations, so that no time may be lost in idle debate. . . . pushing on smartly is the road to success."[3]

Successful Integration of Joint Operating Principles

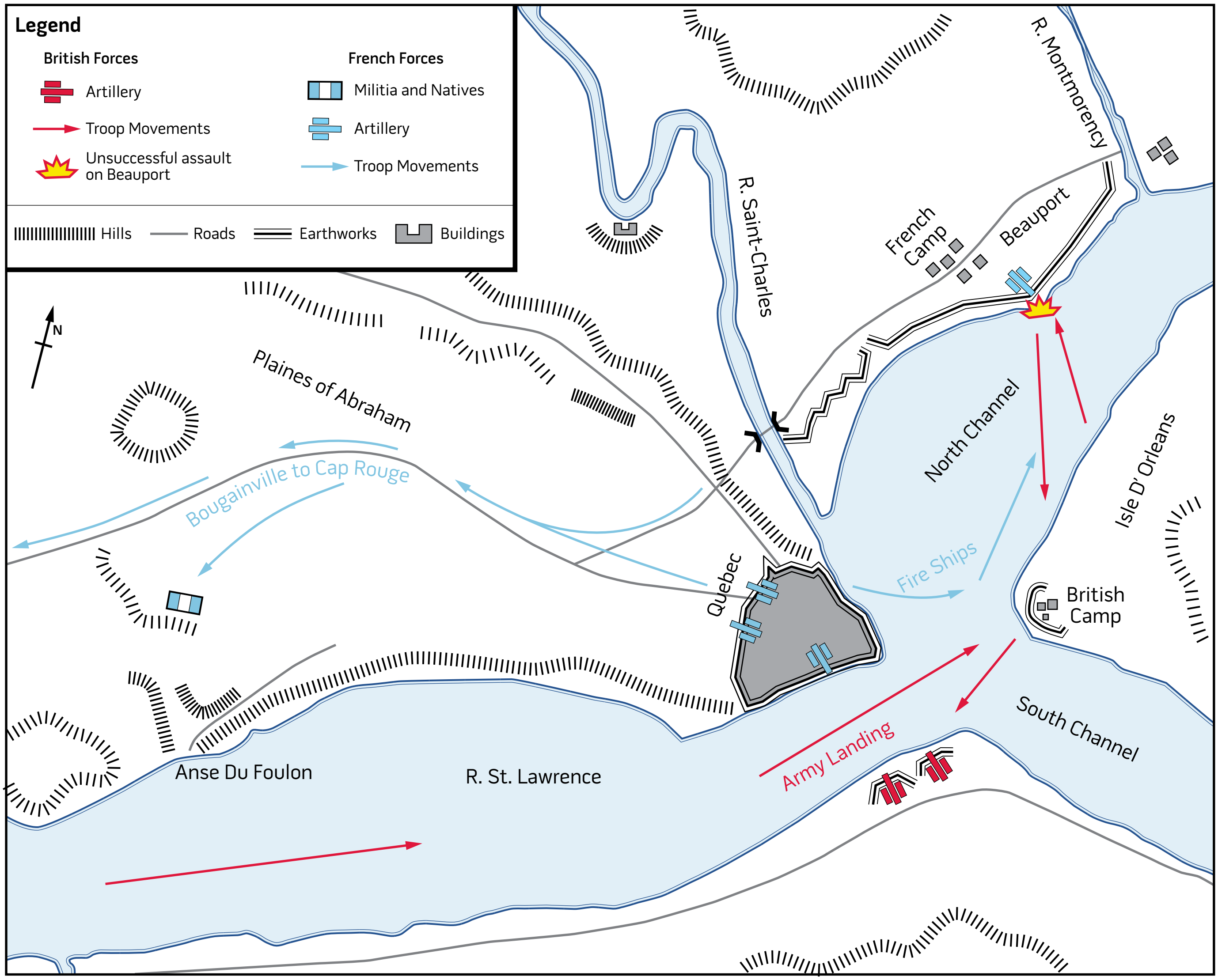
During the Quebec campaign, Wolfe integrated a majority of what we today call the principles of joint operations, using each as a force multiplier for the next, leading to ultimate victory on the Plains of Abraham.

Objective. The British had a clear and concrete strategic objective: the capture of the French Canadian capital of Quebec. This clarity and consistency allowed Wolfe to organize his operational use of joint principles toward a consistent strategic goal. Maintaining this clear and consistent objective served as a prerequisite to leveraging the other joint principles during the campaign.

Unity of Command. Though Britain had no doctrinal concept of jointness, the clarity of the objective encouraged excellent British interservice cooperation at Quebec. Wolfe needed this given his reliance on the navy for access to French Canada and for overall campaign maneuver. British Admiral Charles Saunders reported that "during this tedious campaign, there has continued a perfect good understanding between the army and navy." George Townshend, one of Wolfe's brigadiers, acknowledged that "we are indebted for our success to the constant assistance and support received from [the admirals]."[4]

Economy of Force. During the campaign Wolfe wrote, the "Marquis de

Figure 1. Siege of Quebec during June 28–31, 1759



(Courtesy Hoodinski)

Montcalm is at the head of a great number of bad soldiers, and I am at the head of a small number of good ones."[5] Wolfe sought to besiege his enemy, despite being heavily outnumbered throughout the province. He relied on the fact that his British regulars were well drilled and well disciplined and that most British battalions at Quebec had trained extensively the year before in joint army-navy amphibious tactics.[6] This greatly reduced the significance of simple numerical inferiority, especially because Wolfe's retention of the initiative would allow him to concentrate his limited forces against the primary effort.

Offensive. Wolfe did seize the initiative, although his initial attack at Montmorency utterly failed and cost 440 casualties.[7] Wolfe nevertheless retained focus on his objective and remained on the offensive at the operational level when he launched his amphibious assault on September 13. After reaching the promontory of Quebec, however, Wolfe switched to the tactical defensive, waiting patiently for Montcalm to attack and giving tactical initiative to the French.[8] While this move violated the broad principle of the offensive, it did further Wolfe's campaign goal of drawing Montcalm into open battle and embodied the modern instruction to joint officers that "commanders adopt the defensive only as a temporary expedient."[9] After the decisive engagement on the Plains of Abraham, British forces switched back to the operational offensive for the remainder of the campaign.

Maneuver. By exploiting unity of command and economy of force, Wolfe could pursue the offensive with remarkable skill by employing maneuver and making use of military geography. Relying on the navy's direct observations of the tidal pattern of the St. Lawrence River, Wolfe selected the one night in September 1759 when the tides would deliver his men—who embarked at 0200 on the morning of September 13—to the target Anse au Foulon at 0400, shortly before dawn. Given tidal conditions, an amphibious operation the night before would land his men a full hour before dawn; one the following night would fail to deliver them ashore until after dawn. Additionally, Wolfe took advantage of moonlight to enable his assault to navigate successfully but without detection. The southeasterly direction of the moonlight effectively lit up the northern shore for his ships to identify their landing area, but failed to silhouette his assault force until it reached the objective—thereby denying the French sentries effective surveillance until nearly the last moment.[10] Then British troops climbed a 175-foot bluff where they overpowered the small number of French defenders.[11] This masterful use of maneuver further demonstrated that a commander must tailor abstract operational principles to concrete physical and temporal conditions.

Surprise. The well-executed British maneuver produced total surprise among the French. In 1757, Montcalm had identified Beauport, east of Quebec, as "the only place where the enemy can, and must, make their landing."[12] This key assumption blinded Montcalm to Wolfe's actual operational plan even after its initiation. Montcalm's failure to anticipate Wolfe's point of attack reduced Montcalm to developing a battle plan on the spot with poor situational awareness and poor communications with his dispersed forces.

British deception efforts also achieved great success. The day before Wolfe's assault on the Anse au Foulon, Admiral Saunders's sailors placed buoys into the river near Beauport as if to mark obstacles in the St. Lawrence River for an amphibious assault to avoid, as well as to conduct a heavy bombardment there. Three hours before Wolfe's landing upriver, Saunders's men rowed back and forth in the St. Lawrence near Beauport to imply an imminent landing.[13] Montcalm so strongly assumed a Beauport assault that he even interpreted the British ships traveling upriver (with Wolfe's actual amphibious assault force) as itself a diversion from the anticipated main assault at Beauport. Ultimately, Montcalm did not reach the Plains of Abraham until 3 hours after the initial British landing.[14]

Mass. The shock among French leaders led Montcalm to react relatively quickly without waiting for reinforcements, which allowed the mass effects of the British regulars' firepower to become the decisive principle in the French defeat on the Plains of Abraham. Tactically, British officers usually sought to control their men's fire for coordinated effect, whereas the French generally approved of French troops firing on their own, favoring efforts to follow this fire with a quick bayonet charge.[15] The French forces roughly equaled the number of British forces in the battle, despite Montcalm's decision to strike before Bougainville's nearly 2,000 reinforcements arrived. While French regulars had the discipline to advance deliberately and hold ranks, the Canadian militiamen sprinkled throughout the French units broke into a run. Various French forces opened fire far outside musket range, at about 125 to 150 yards, to minimal effect. French regulars reloaded standing in line while the militia reloaded in their traditional method—under cover or lying on the ground. The effect left the French line completely uneven and incapable of massing fire effects.[16] As the French advanced, the center of the line pulled ahead and the left fell behind, creating three distinct clusters of French units as they approached the British lines.[17] Once French troops started to fire their muskets, the French battalions effectively split into small groups of regulars or militia, given their different methods of reloading.[18]

British forces held fire as the French advanced; British units on the flanks opened fire at a range of 60 yards, but units in the center opened fire simultaneously at 40 yards with devastating effect.[19] A British officer reported that British forces "with great calmness, as remarkable a close and heavy discharge, as I ever saw . . . and, indeed well might the French Officers say, that they never opposed such a shock as they received from the center of our line, for that they believed every ball took place" during the decisive engagement on the Plains of Abraham. Once the smoke cleared, British forces could see the French force in full retreat.[20]

Current doctrinal instructions to joint officers caution that "the principles do not apply equally in all joint operations."[21] When Wolfe applied lessons learned from historical cases and his own experiences throughout the campaign, he reinforced the concept of operational command as an *art*, requiring commanders to interpret the relative weight of joint operating principles and their use in appropriate combinations. In this case, knowing when and how to violate specific principles actually allowed Wolfe to accomplish his overall campaign goals.

Security. Wolfe intentionally violated the principle of security at the climactic point of the battle by stationing his troops in a static line on the Plains of Abraham without entrenching and with no viable escape route. This had the calculated effect of showing enough apparent vulnerability to provoke Montcalm finally into what Wolfe had sought all summer: an open-field, pitched battle.[22] By sacrificing the principle of security, Wolfe was able to set up conditions to exploit the principle of mass to decisive effect.

Simplicity. Wolfe also jettisoned the principle of simplicity, relying instead on a highly risky, highly coordinated, and tightly timed joint service operation. Part of this decision rested on his supreme confidence in his military and naval force capabilities. The remainder reflected Wolfe's view "that in war something must be allowed to chance and fortune, seeing that it is in its nature hazardous, and an option of difficulties."[23] Additionally, the sheer complexity of the operation helped to guarantee that the French would not anticipate it and that Wolfe could exploit the principle of total surprise.

Perseverance. Wolfe did not focus at all on the three newer principles (perseverance, legitimacy, and restraint) beyond the traditional principles of war. Abandoning perseverance, he wisely took a major gamble to bring the campaign to a conclusion in September because waiting would have deprived Wolfe of his greatest military advantage, British naval mobility. Waiting also would have risked the primary British objective—to capture Quebec City during 1759.[24]

Legitimacy. Wolfe also did not concern himself with the principle of legitimacy. As a regular army officer fighting in a declared war, Wolfe made no special effort to demonstrate legitimacy to the French or French Canadians. Wolfe, who respected well-trained regular troops, disdained even his own American colonial troops, calling them "the dirtiest most contemptible cowardly dogs that you can conceive."[25] None of this contempt for the principle of legitimacy had any apparent effect on Wolfe's campaign progress.

Restraint. Additionally, during the combat phase of the operation, Wolfe grossly violated the principle of restraint in a failed attempt to provoke Montcalm into open battle. After the British failure at Montmorency in July, Wolfe ordered his forces "to destroy the Harvest, Houses, & Cattle" of the French Canadian countryside, whereupon British troops laid waste to 1,400 civilian farms.[26]

By contrast, Wolfe's successor Townshend realized that after the end of combat operations, he did not have enough forces to control a hostile French Canadian civilian population. When the remaining French garrison in Quebec surrendered, he ordered that "all acts of violence, pillage, & cruelty are strictly forbid [*sic*]. The garrison are to have the Honours of War."[27] Britain committed to returning French regulars to France under flag of truce, while allowing Canadian militiamen who surrendered their arms and pledged fidelity to Britain to return home.[28] In this way, the British maintained a successful occupation of Quebec City, demonstrating that while restraint had minimal relevance during combat operations, it had a decisive importance as part of postcombat stabilization efforts.

Montcalm's Ineffective Use of Joint Operating Principles

Montcalm's failure to integrate the principles of joint operations during the Quebec campaign, in contrast to Wolfe's efforts, serves as a cautionary tale to joint officers about the risks of applying these principles in isolation. By the time of Wolfe's Quebec campaign, Montcalm had to function on the operational defensive with limited personnel and material resources, since France had reoriented its strategic priorities in the wider war toward Europe and away from Canada.[29] This reality elicited a general defeatism in Montcalm by early 1759 when he predicted that "Canada will fall to the English, maybe this campaign, or the next."[30] Acting on the operational defensive put Montcalm at a significant disadvantage, ceding the initiative to Wolfe's forces. This restricted Montcalm to a reactive approach and led to a haphazard application of the principles of joint operations throughout the campaign, which in turn led to general operational incoherence and, ultimately, French defeat.

Objective. Montcalm demonstrated strategic clarity regarding his campaign objective, viewing his primary task as the conventional military defense of Quebec City, which held the key to French control of Canada. This held true throughout the campaign despite Montcalm's strategic disagreement with the French Canadian governor General Marquis de Vaudreuil, who believed that even if the British captured the city, they could not hold it if French and allied Native forces retained the ability to conduct guerrilla-style harassment throughout the province.[31] Since both the French and British commanders identified control of the capital as the campaign's key objective, this parallel focus intensified the importance for each of effectively integrating the remaining operational principles.

Perseverance. Montcalm did exercise perseverance but generally by default rather than calculation. During the campaign, Montcalm had the luxury of time and demonstrated perseverance by refusing to allow the British to draw him from his strong defensive positions from late June through early September.[32] This negatively affected the overall campaign, however, since it occurred only because Montcalm surrendered the more decisive principle of the offensive.

Simplicity. As with the principle of perseverance, Montcalm exercised the principle of simplicity, but in a manner similarly divorced from the other principles. Originally, Montcalm settled on a straightforward preparation of his defenses while waiting for likely British assaults on his positions. Once British forces arrived at the Plains of Abraham, Montcalm ordered a straightforward frontal assault on the British lines, dictated mostly by the topography of the Plains of Abraham.[33] In this case, though, the simplicity of Montcalm's attack derived more from immediacy than from wisdom, and even then it illuminated a lack of interoperability between French regular and Canadian militia units.

Legitimacy. Montcalm, like Wolfe, did not show great concern for the principle of legitimacy and, similar to Wolfe, suffered no apparent drawbacks for it. The French court's order early in 1759 elevating Montcalm to the position of commander in chief of all French forces in Canada did head off any potential infighting between Montcalm and French Canada's political leadership over strategic direction.[34] Montcalm, though, had little sympathy for his French Canadian comrades. When some French Canadian civilians in the summer of 1759 suggested surrendering the capital in order to terminate Wolfe's campaign of destruction in the countryside, Montcalm threatened them with abandonment to "the savages" as a form of counterterror.[35] Nevertheless, Montcalm still managed to exercise effective operational authority among his French regulars and his Canadian militia units during the campaign.

Unity of Command. Montcalm did exercise unity of command in Canada better than his French contemporaries in Europe. The court at Versailles, which consistently made binding "suggestions" to its field commanders, could not micromanage military actions in Canada due to physical distance.[36] Montcalm therefore exercised direct control over French regulars and Canadian militia. He did not exercise it, however, over France's Native allies, who numbered over 1,000 warriors in the Quebec campaign. The

"View of Louisbourg when the city was besieged by British forces in 1758," Captain Charles Ince, drawn on the spot, engraved by P. Canot, November 11, 1762 (Courtesy Yale Center for British Art, Paul Mellon Collection)

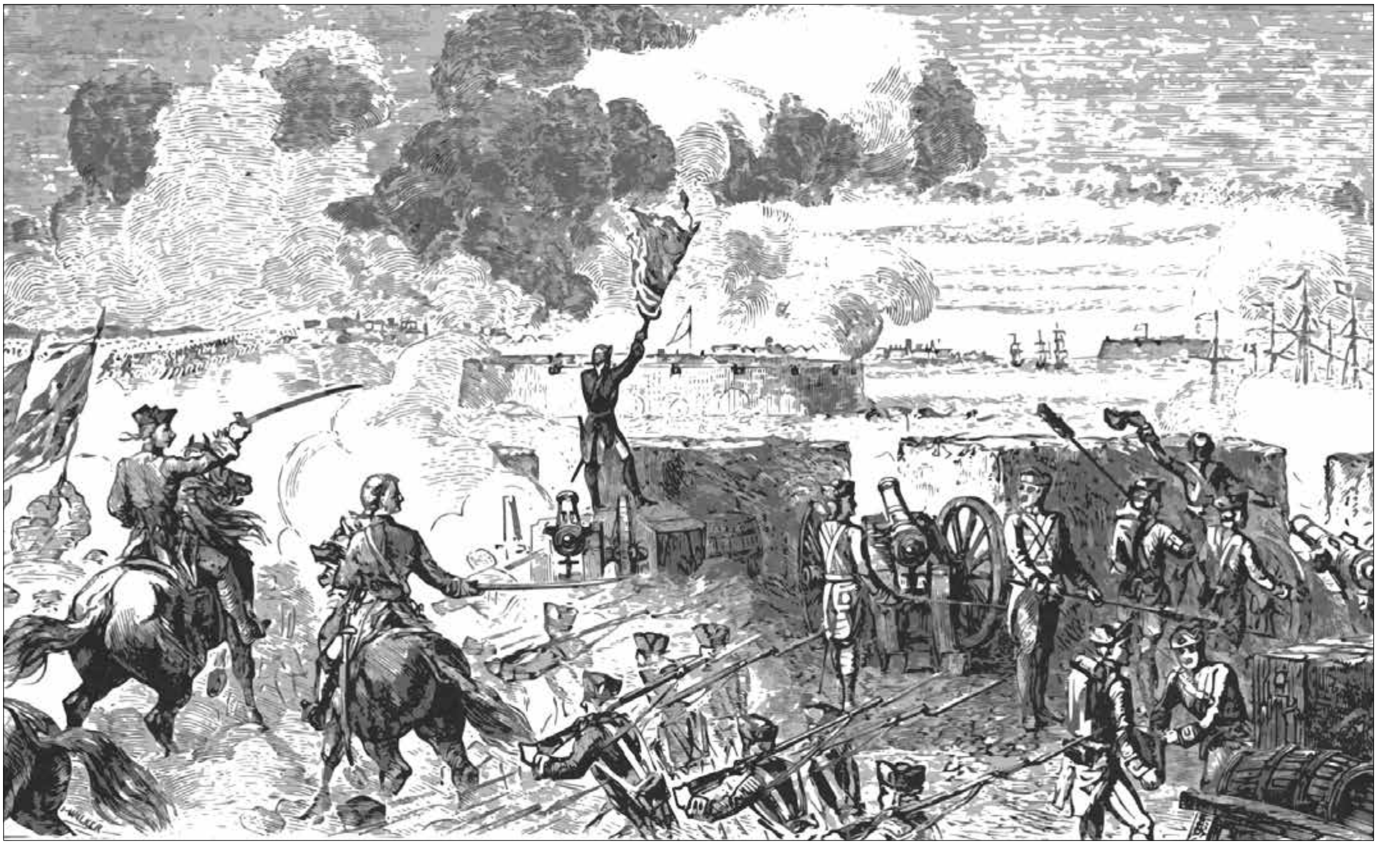
Native allies traditionally fought in parallel, rather than integrated, efforts with the French, and they performed effectively against the British at the Plains of Abraham—British troops had established themselves in a field surrounded by trees and brush, and this provided Native skirmishers with an ideal operating environment.[37]

But on the day of the battle, French unity of command broke down. Montcalm and both of his acting brigadiers suffered mortal wounds, meaning that the Quebec garrison after the battle had no senior French commanders. Meanwhile, the remaining French forces outside the city, now under Governor-General Marquis de Vaudreuil's nominal command, decided after a council of the remaining officers to abandon the city to the British siege.[38]

Security. Montcalm practiced security commendably throughout the campaign except for one disastrous oversight. He heavily fortified the area east of Quebec with French regulars, which allowed him to repel Wolfe's attacks in July, but relied on less capable militia units west of Quebec given the French expectation that the British would not land there.[39] Montcalm's heavy fortification of the Beauport area, Wolfe's preferred amphibious target, did in fact deter Wolfe from landing there.[40] The French commander, though, demonstrated a fatal overconfidence that the 60-yard cliff from the river to the promontory of Quebec afforded a natural defense west of the city where "100 men posted there could stop a whole army [and] give us the time to wait for daylight [and] march there from [Beauport]." French overconfidence also led them to neglect the establishment of a signals or mounted courier system to allow the small garrison to call for help quickly.[41]

Restraint. As with the principle of perseverance, Montcalm's exercise of restraint derived more from his defensive posture than as an integrated operational approach to achieve an objective. Montcalm also fought among a friendly population, which restricted any temptation to violate restraint. But he abandoned this prudence once British troops appeared outside Quebec, allowing Wolfe to provoke him rapidly into a disadvantageous military engagement.[42] Montcalm's failure to show restraint in waiting for reinforcements on the Plains of Abraham contributed heavily to his defeat.

Economy of Force. Because Montcalm remained on the operational defensive, he dispersed his forces over a wide geographic area, thereby violating the principle of economy of force. Since the British could decide the location of the primary engagement, this guaranteed that the French force would expend a high proportion of its combat power on secondary efforts. Wolfe's assault, therefore, caught French forces widely dispersed—Montcalm to the east at Beauport, Bougainville to the



"Brigadier General James Wolfe at the siege of Louisbourg, 1758," by Charles R. Tuttle (*Illustrated History of the Dominion*, 1877)

west at Cap Rouge—and as a result, Bougainville and 2,000 of France's best troops did not arrive on the battlefield until after the British had defeated Montcalm's main force.[43]

Maneuver. Montcalm lost control of the St. Lawrence River east of Quebec City at the start of the campaign.[44] This, plus his need to defend a broad territory, severely limited his ability to maneuver his forces. Ultimately, Montcalm's need to move his forces by land in the operational area meant that first his own and then Bougainville's forces each arrived too late to the battle to repel British forces.[45]

Surprise. Montcalm failed most disastrously on the interrelated principles of surprise, offensive, and mass. At the Plains of Abraham, Montcalm suffered total surprise regarding the location and timing of the British assault, which arguably led to his rash and unsuccessful response. Conversely, Montcalm's behavior achieved no surprise while playing perfectly into Wolfe's operational plan, meaning the British did not have to adjust their approach at all due to French actions.

Offensive. Montcalm spent the entire campaign on the operational defensive and never achieved the initiative throughout the campaign. When Montcalm suddenly decided to switch without preparation to the tactical offensive on the Plains of Abraham, he did this solely as a reaction to Wolfe's initiative. This combination, which proved catastrophic, demonstrates that applying a joint operating principle in a technical way without integrating it into an overall operational context can actually do more harm than good.

Mass. Montcalm's offensive action also suffered from a fatal weakening of French mass both before and during the battle. Because most battalions of French regulars had suffered attrition over the course of previous North American campaigns with few replacements from Europe, Montcalm compensated by integrating Canadian militia into French regular units, thus reducing unit integrity across many of his regular forces.[46] Montcalm compounded this weakness by failing to wait for Bougainville to arrive with the best French regular units available to his command before launching his attack on the British line. The disjointed French attack displayed a critical French failure to concentrate mass among French combat power, leading to decisive defeat.

Conclusion

Wolfe's experience at Quebec implies that while formal doctrinal instruction in the principles of joint operations is useful, it will not by itself yield superior integration of these principles in practice. A truly inspired application of joint operating principles requires a commander to rely on a broad understanding of historical case studies, personal experience, creativity, and specific campaign conditions to exploit these principles to maximum effect. Conversely, Montcalm's experience suggests that enacting these principles simply as part of a rote checklist might individually yield modest results but will fail to maximize a military force's capabilities and will leave the force at the mercy of an adversary commander who integrates these principles into a coherent overall operational plan. Notably, Wolfe favored historical authors who were not only military theorists but also military practitioners.

Today's military practitioners can benefit from Wolfe's example of an abiding focus on the overall objective of the French capital, his mastery of surprise through understanding of the terrain, and his unique massing of overwhelming effects. While the character of war may be rapidly evolving, the nature of war maintains many immutable principles. Studying historical cases demonstrates that the principles of joint operations apply universally in time and place, a lesson James Wolfe implicitly knew and mastered in 1759. Future joint force officers will face the challenge to fuse doctrinal understanding, historical exemplars, and personal creativity to apply joint operating principles in the future operating environment. **JFQ**

Notes

[1] Walter R. Borneman, *The French and Indian War: Deciding the Fate of North America* (New York: HarperCollins, 2006), 204, 207, 211–213, 217–223; William M. Fowler, Jr., *Empires at War: The French and Indian War and the Struggle for North America, 1754–1763* (New York: Walker and Company, 2005), 184, 191–194, 199–200, 204–213.

[2] B.H. Liddell Hart, *Great Captains Unveiled* (London: Greenhill Books, 1989), 242–246.

[3] Ibid., 212–213, 245, 247–250.

[4] Simon Foster, *Hit the Beach! Amphibious Warfare from the Plains of Abraham to San Carlos Water* (London: Arms and Armour Press, 1995), 20.

[5] Fowler, *Empires at War*, 198.

[6] Stephen Brumwell, "General Wolfe's Men in Quebec," *History Today* 59, no. 9 (September 2009), 48–51.

[7] Stuart Reid, *Quebec 1759: The Battle That Won Canada* (Oxford: Osprey Publishing, 2003), 42.

[8] Fred Anderson, *Crucible of War: The Seven Years' War and the Fate of Empire in British North America, 1754–1766* (New York: Knopf, 2000), 357.

[9] Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017, incorporating change 1, October 22, 2018), A-3.

[10] Donald W. Olsen et al., "Perfect Tide, Ideal Moon: An Unappreciated Aspect of Wolfe's Generalship at Quebec, 1759," *The William and Mary Quarterly* 59, no. 4 (October 2002), 965, 967, 969, 973–974.

[11] Anderson, *Crucible of War*, 353–354.

[12] D. Peter MacLeod, *Northern Armageddon: The Battle of the Plains of Abraham and the Making of the American Revolution* (New York: Knopf, 2016), 70.

[13] Borneman, *The French and Indian War*, 219; see also Anderson, *Crucible of War*, 355.

[14] Anderson, *Crucible of War*, 355–356.

[15] Reid, *Quebec 1759*, 74.

[16] Anderson, *Crucible of War*, 360–361.

[17] MacLeod, *Northern Armageddon*, 191.

[18] Ibid., 195.

[19] Anderson, *Crucible of War*, 360–361.

[20] Reid, *Quebec 1759*, 75.

[21] JP 3-0, A-1.

[22] Anderson, *Crucible of War*, 355.

[23] Liddell Hart, *Great Captains Unveiled*, 250.

[24] Frank W. Brecher, *Losing a Continent: France's North American Policy, 1753–1763* (Westport, CT: Greenwood Press, 1998), 149.

[25] Ibid., 255.

[26] MacLeod, *Northern Armageddon*, 40; see also Anderson, *Crucible of War*, 344.

[27] MacLeod, *Northern Armageddon*, 267.

[28] Anderson, *Crucible of War*, 364–365.

[29] Francis Parkman, *France and England in North America*, vol. 2, part 7*: Montcalm and Wolfe* (Boston: Little, Brown, and Company, 1942), 183.

[30] MacLeod, *Northern Armageddon*, 189–190.

[31] Anderson, *Crucible of War*, 346.

[32] Fowler, *Empires at War*, 198, 206–207.

[33] Anderson, *Crucible of War*, 359.

[34] Borneman, *The French and Indian War*, 190.

[35] Francis Jennings, *Empire of Fortune: Crowns, Colonies, and Tribes in the Seven Years War in America* (New York: Norton, 1988), 421.

[36] Lee Kennett, *The French Armies in the Seven Years' War: A Study in Military Organization and Administration* (Durham: Duke University Press, 1967), 19–21.

[37] MacLeod, *Northern Armageddon*, 66–68, 172–173.

[38] Anderson, *Crucible of War*, 363–364.

[39] Ibid., 348.

[40] MacLeod, *Northern Armageddon*, 28.

[41] Reid, *Quebec 1759*, 61; see also MacLeod, *Northern Armageddon*, 158.

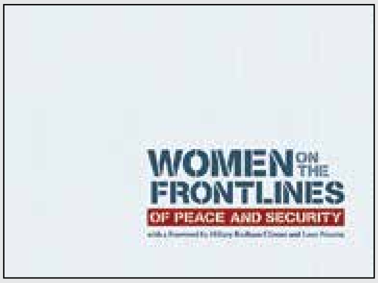
[42] Fowler, *Empires at War*, 198, 206–207.

[43] Borneman, *The French and Indian War*, 220–221.

[44] Brecher, *Losing a Continent*, 135–136.

[45] Ibid., 220–221.

[46] Reid, *Quebec 1759*, 17.



From NDU Press

Women on the Frontlines of Peace and Security

Foreword by Hillary Rodham Clinton and Leon Panetta

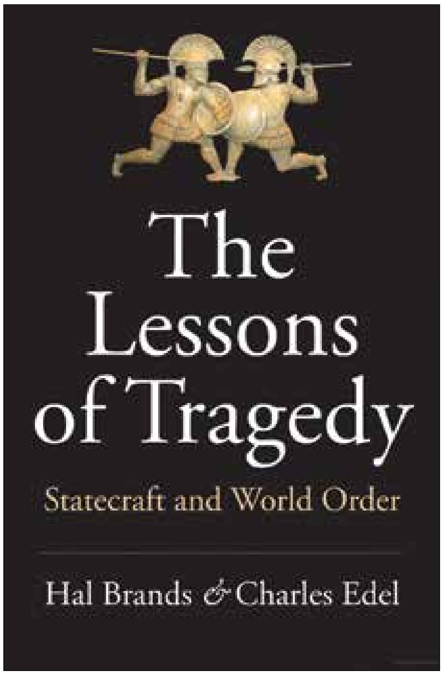
NDU Press, 2015 • 218 pp.

This book reflects President Barack Obama's commitment to advancing women's participation in preventing conflict and keeping peace. It is inspired by the countless women and girls on the frontlines who make a difference every day in their communities and societies by creating opportunities and building peace.

When women are involved in peace negotiations, they raise important issues that might be otherwise overlooked. When women are educated and enabled to participate in every aspect of their societies—from growing the economy to strengthening the security sector—communities are more stable and less prone to conflict.

The goal of this book is to bring together these diverse voices. As leaders in every region of the world recognize, no country can reach its full potential without the participation of all its citizens.

Available at ndupress.ndu.edu/Books/WomenontheFrontlinesofPeaceandSecurity.aspx



The Lessons of Tragedy: Statecraft and World Order

By Hal Brands and Charles Edel
Yale University Press, 2019
200 pp. $25.00
ISBN: 978-0300238242

Reviewed by Joseph J. Collins

The field of international relations is awash with books on world order, "the system of norms, rules, and power relationships that regulates international affairs" (p. 42). While military concerns often focus on technical or operational issues, senior officers and strategists need to understand the evolving world order to understand the strategic context that underpins their work.

Hal Brands, the Henry Kissinger Professor of Global Affairs at The Johns Hopkins School of Advanced International Studies, and Charles Edel, a senior fellow in the United States Studies Centre at the University of Sydney, Australia, have sought the wisdom of the past to help us understand the future world order. Their thesis is that tragedy has been a recurring but not inevitable part of international affairs. To understand world politics, one must be alert to the potential for tragedy. Sadly, the United States today has lost its tragic sensibility at a time when it must work with purpose and vigor to shore up a faltering world order. In the process of proving this thesis, the two authors have published a book that is relatively comprehensive, well-written, and original in its approach.

The authors begin with Aristotle, who noted that a tragic sensibility is about understanding "not the thing that has happened but a kind of thing that might happen" (p. 3). The citizens of volatile Greek city-states had a much better sense of what could happen at the extremes of state relations, but Americans, the authors argue, are "serial amnesiacs." After 75 years of peace among the major powers, Americans "are losing their sense of tragedy" (p. 5). The authors assert that Americans "must re-discover their inner sense of tragedy *before* they have to experience it themselves" (p.6, emphasis in the original). Who better to teach Americans about tragedy than the ancient Greeks, who invented the art form more than 20 centuries past?

The ancient Greeks warned against both hubris and complacency. Blending fact, fiction, and recreation, their plays often shocked the audience into contemplating a contemporary world in relation to tragedies of the past. The authors offer as a prime example Aeschylus's dissection in *The Persians* of how Xerxes abused his superior capabilities and underestimated his determined Greek opponents. Persian hubris ruled, and "dangers abound when leaders reach beyond their grasp" (p. 14). Greeks and Persians paid heavily for Xerxes' folly. The high prices paid by Americans and the indigenous people in the invasion of Iraq and the war in Vietnam were prefigured by the price paid by Greeks and Persians. Unfortunately, the Greek ability to learn from tragedy was not perfect; their refined tragic sensibility did not prevent them from initiating the disastrous Peloponnesian War 50 years later.

As the eras unfolded, progress and development had their day, but tragedy, riding in the trains of large-scale wars, made repeat appearances. The Thirty Years' War, the Napoleonic Wars, and World War I all had increasingly tragic outcomes. The authors worry that today the potential for great power conflict appears to be growing as the proclivity of Western powers to take collective action is fading. The last time that happened was in the late 1930s, where the high casualties of World War I, isolationism, the prominence of idealistic thinking, and poor economic conditions induced paralysis among the Allies in the face of the Axis threat.

The post–World War II period was grounded in the lessons of the tragedy of that greatest of all conflicts. The United States and its Allies created a comprehensive world order that included security organizations, trade rules, monetary policy management, a developmental assistance bank, and the United Nations system. Still, the bipolar competition between the United States and the Soviet Union accommodated limited wars and proxy conflicts. Wars of national liberation, often aided and abetted by the Soviet Union or China, were frequent, but great power war was avoided. Prosperity returned to the developed world, and economic progress spread in the developing world. The potential for tragedy faded in the American mind.

Brands and Edel argue that after 75 years of great power peace, the United States has lost the tragic sensibility that "impelled it to do great things—and in doing so, it is undermining the exertions that have long held tragedy at bay" (p. 91). The end of the Cold War, the desire for a peace dividend, idealistic "end of history" thinking, and a real reduction in defense spending all took place before the costly wars in Afghanistan and Iraq. After nearly a decade of fighting the unanticipated war on terror, the United States endured a serious financial crisis. At the same time, China and Russia had become more powerful and aggressive internationally. In 2008, the Russians invaded Georgia. A half-decade later, they seized the Crimea and invaded Ukraine. In 2017, Chinese Premier Xi Jinping told the Party Congress that China could now "take center stage in the world" (p. 131) and potentially establish a Sinocentric world order.

The United States, according to the authors, faces a "darkening horizon" and increasingly "contested primacy" (p. 123). The onset of the Trump Presidency has complicated the U.S. response, weakening the strong U.S. alliance focus, and detracting from its propensity to exercise international leadership. The potential for great power conflict today is higher than it has been since the Cold War. Were that not enough to worry about, Iran and North Korea provide additional sources of regional instability. The authors compare the contemporary period to the late 1930s and assert that today's defenders of world order "seem demoralized, divided, and unreliable" (p. 140).

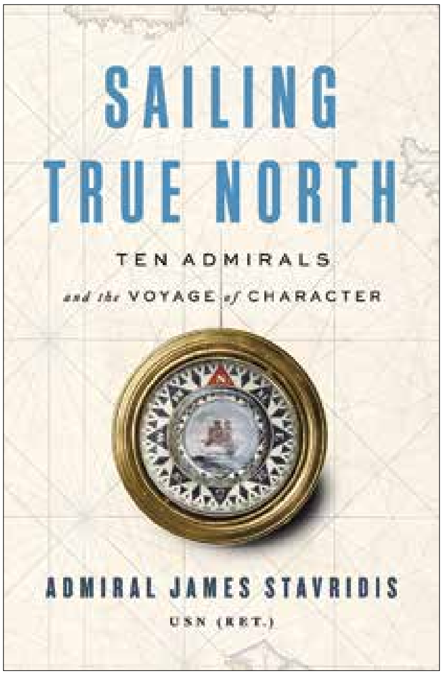
In the final chapter of the book, Brands and Edel summarize their argument and leave the reader with what amounts to a set of conceptual recommendations. They remind us that tragedy in international politics is normal and that today tragedy is "again stalking global affairs" (p. 149). At the same time, they reject both complacency and fatalism. All is not lost. To repair the world order, they recommend collective action and communal sacrifice. This will require consistent U.S. leadership, which they believe has been lacking for many years. The authors recommend "timely and enduring action" (p. 158) to solve both immediate and unending long-term problems. Finally, they recommend a sense of restraint and proportion, avoiding both complacency and hubris, which just happens to be a central message of Greek tragedies.

The Lessons of Tragedy is an excellent book, but the analysis is focused on great power politics. The centrality of survival and security supports that approach, but the fraying of the international order has a number of important aspects beyond interstate security politics. The issues of international political economy, trade, globalization, and regional/global organizations are a big part of the world order story, as are Chinese and Russian futures, critical metrics in appreciating the potential for tragedy.

The curious reader may want to cast a wider net on the issue of world order. Three new books that would be useful are Kori Schake, *America vs. the West: Can the Liberal World Order Be Preserved* (Penguin Specials, 2018); Robert Kagan, *The Jungle Grows Back: America and Our Imperiled World* (Knopf, 2018); and Michael Mazarr and Ashley Rhoades, *Testing the Value of the Postwar International Order* (RAND, 2018).

But if you have a chance to read only one book on world order, you would do well to read and meditate on *Lessons of Tragedy*. Aristotle would salute your prudence. **JFQ**

Colonel Joseph J. Collins, USA (Ret.), Ph.D., taught for 25 years at the U.S. Military Academy at West Point, the National War College, and Georgetown University. From 2001 to 2004, he served as the Deputy Assistant Secretary of Defense for Stability Operations. He holds a doctorate in political science from Columbia University and is a life member of the Council on Foreign Relations.



Sailing True North: Ten Admirals and the Voyage of Character

By James Stavridis
Penguin Press, 2019
336 pp. $28.00
ISBN 978-0525559931

Reviewed by Peter H. Daly

Character is being widely discussed on the national stage today, and it is the main subject of *Sailing True North: Ten Admirals and the Voyage of Character*. This new title spans the arc of time from Themistocles to current-day admirals. For each of his subjects, the author distills their stories and key attributes. I have known Jim Stavridis for more than 30 years and most recently worked closely with him in my role as CEO and Publisher at the U.S. Naval Institute when he was Chair of the Board.

The short histories and examples that he provides in *Sailing True North* do not just focus on successes; the book does a good job of giving balanced treatment to both successes and failures. The flaws are covered, and from these flaws and failures, we learn the most. It is a heavy lift to see so many historic subjects in one title and relate these to the present-day world, all while providing relatable examples within the author's own substantial experience. *Sailing True North* makes the lift and does it well.

In reading the work, I was reminded of the writings of Douglas Southall Freeman, best known for his biographies of George Washington (Simon & Schuster, 1995) and Robert E. Lee (Scribners, 1991). Freeman gave a series of lectures at the Army War College and the Naval War College that I recommend to anyone who wants to understand leadership under stress and under truly consequential circumstances. After looking at the leadership traits common to these men and others he studied, Freeman summed up their leadership qualities in three tenets, which in today's diverse world of military service would translate as follows: "Know Your Stuff," "Do the Right Thing," and "Look After Your People."

Leadership and character are always important, but perhaps even more so now. There is a real thirst for national leadership—on both sides of the aisle—that citizens can feel proud of. This book proves that leadership is not limited to heroic seagoing assignments, even in the Navy. Stavridis highlights three examples in particular: Alfred Thayer Mahan, the writer whose books about seapower, history, and geopolitics continue to influence our ideas about foreign policy and national defense; Hyman Rickover, the visionary whose work on nuclear propulsion transformed the Navy forever; and Grace Hopper, the gifted mathematician and computer scientist who led the Navy into the computer age. These leaders demonstrated the kind of character—especially the dedication to national service—that Stavridis obviously admires.

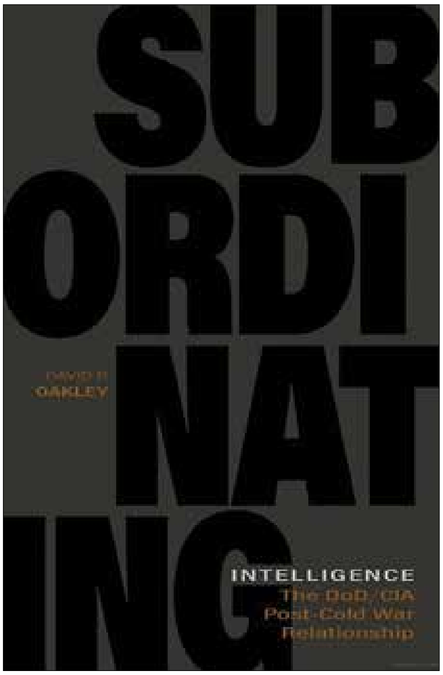
Another context that makes this book timely is the dramatically changed media environment. Deliberate disinformation and the polarization of debate and discourse make it more difficult for citizens to distinguish factual information from false. The media environment is weaponized, and a casualty of this is a loss of faith in our leaders and our institutions. We crave the "essential sanity" that Freeman identified in George Washington. A malaise has set in—one that manifests itself in a trend of the best and brightest being discouraged from engaging in national service.

While its emphasis is on naval leaders, Stavridis's book provides character and leadership insights that transcend things naval and are relevant to the joint warfighting community and joint professional military education. Indeed, it has lessons that extend well beyond the purely military realm. This gives *Sailing True North* a Freeman-esque quality and utility, and I recommend it to anyone who wants to understand the essential questions of character and leadership under stress. Jim Stavridis boils down the traits, the common threads. For each, the author provides examples from his own experience. At the top of his list of 10 key conclusions are creativity followed by resilience. The book makes readers think and challenges us to ask who our heroes are and what qualities they embody. Stavridis encourages us to self-examine as we make our voyage through life with all the tests of leadership and character that one will experience.

The author is supremely well read, and, as such, he provides an invaluable distillation of a vast span of history for easy assimilation. I found the style and the structure of the book easy to follow and enjoyable to read. Translating this history and these traits into specific, modern examples makes the book both an invaluable primer for new students of leadership and a stepping off point for those who want to delve deeper into specific historical subjects.

This book answers the question: What does Jim Stavridis think is most important? When the author is this well read, this well known, and himself served at the most consequential levels of command, that is a question worth answering. This makes it a recommended read—a must read. JFQ

Vice Admiral Peter H. Daly, USN (Ret.), is the Chief Executive Officer of the U.S. Naval Institute.



Subordinating Intelligence: The DOD/CIA Post–Cold War Relationship

By David P. Oakley
University Press of Kentucky, 2019
264 pp. $37.70
ISBN: 978-0813176703

Reviewed by J. Paul Pope

Long experiences in Iraq, Afghanistan, and other conflicts have resulted in an increased emphasis on civil-military relationships and the interagency community in U.S. doctrine. Predeployment training now includes exercises requiring coordination with Embassies, Ambassadors, and U.S. and international agencies. Harnessing, aligning, and integrating the collective expertise and capabilities found in these organizations is essential for mission accomplishment. This integration cannot be assumed in mission planning; it requires closer coordination than previously understood, mutual understanding, and intentionality at all levels.

The practical record shows we have too often failed to achieve even basic mission alignment or deconfliction. But beyond an exhortation to expand our collective understanding of jointness, how does this actually work? Why is it so hard? Who is responsible for making it happen? Who works for whom? *Subordinating Intelligence: The DOD/CIA Post–Cold War Relationship* represents an important contribution to the body of literature on joint operations in this interagency context.

Other intelligence and non-intelligence organizations are important to military operations, but the Central Intelligence Agency is a particular case. In some recent instances, CIA was the only U.S. organization already operating in a region where the Department of Defense (DOD) was assigned a combat mission, as was the case in Afghanistan after 9/11. In noncombat zones, chiefs of station are tasked by the CIA director and the Director of National Intelligence with coordinating all intelligence operations in-country. CIA analysts guard their independence stubbornly, and commanders from William Westmoreland to David Petraeus have found themselves frustrated by the effect their analysis had on the civilian leadership's framing of "their war." Professional development often does too little to prepare rising officers to work with CIA in the field or at senior staff levels, with the recent exception of special operations forces.

Subordinating Intelligence is a well-written analysis of the evolution of the relationship between DOD and CIA in the post–Cold War era. One valuable contribution from this history is the identification of the barriers to cooperation, which pop up time after time in the various instances Oakley describes. A second contribution is the isolation of the factors that made a difference where integration *was* achieved. As implied in the title, however, Oakley's book addresses another important and specific question. CIA was created to be an *independent* agency outside any Cabinet-level department and a *strategic intelligence* organization to serve the needs of the President and the National Security Council.

Oakley sees a threat to this mission based on the creeping militarization of U.S. foreign policy, including explicit and implicit demands that CIA be subordinated to a support role for DOD (despite its immense intelligence resources). An interesting quality of the book is that it is a Soldier—who understands the potential value of CIA capabilities when employing U.S. combat power—who articulates the potential costs of sacrificing its strategic collection and analytic responsibilities to DOD's "infinite demands on a finite resource." Oakley not only illustrates this "support-to-supported" tension for particular missions but also highlights instances where one side or the other fails to understand that their missions are actually different. He quotes a CIA officer describing the DOD's expectation of tactical support in its "sprint" to leave Iraq, while the Department of State and CIA were tasked to focus their efforts on a "marathon" to support a stable Iraq. In his excellent concluding chapter, Oakley quotes Senator David Boren (D-OK) musing about the appropriate role for CIA in 2013 by asking, "In the long term, what's more important, Afghanistan or China?"

While bringing this baked-in dilemma into stark relief, Oakley correctly resists the urge to prescribe bold legislative or executive remedies to resolve it. Yes, the CIA exists to collect strategic intelligence, to provide strategic analysis for the President and his key advisors, and to conduct covert action when lawfully ordered to do so. On the other hand, the CIA can bring unique capabilities to the fight and can contribute to the "rich contextual understanding" (as General Stanley McChrystal described it) required for success on complex battlefields. It would be folly either to subordinate CIA to supporting warfighters or to preclude its assistance when Americans are shedding blood. The chapters between the introduction and the conclusion offer examples and practical principles for building effective teamwork and avoiding these draconian choices, while taking advantage of all available capabilities.

Both military and intelligence professionals would be well served to read this excellent book to find examples of what can go wrong, but also what can go right. Consistent with organizational theory, Oakley records instances of interagency conflict, or "storming," which in turn led to "norming," which led to jointly "performing" the mission. His cases show that this process occurred much faster on the second and third attempts. They also highlight that the importance of personal relationships—often forged by shared danger—speak to the necessity for liaison officers, and offer examples of what can happen when mutual respect for the ethos of other organizational players in the shared operational space results in deep trust. The historical examples seem to indicate that this process can be accelerated, but not replaced, by reorganization or imposed process.

Interagency alignment is a prerequisite for success. Oakley's book is a model for more that needs to be written—on DOD and State, the Federal Bureau of Investigation and CIA, U.S. Aid and DOD, and so forth. I highly recommend his book. **JFQ**

J. Paul Pope is Professor of Practice at the LBJ School for Public Affairs and Senior Fellow in the Intelligence Studies Project at the University of Texas at Austin.

Marine Corps cryptologic analyst assigned to 1st Radio Battalion, I Marine Expeditionary Force Information Group, monitors electromagnetic spectrum during training in support of Command Post Exercise at Marine Corps Base Camp Pendleton, California, December 12, 2018 (U.S. Marine Corps/Brendan Mullin)

Unmasking the Spectrum with Artificial Intelligence

By Matthew J. Florenzen, Kurt M. Shulkitas, and Kyle P. Bair

Imagine you are a combatant commander (CCDR) equipped with the latest capabilities today's military has to offer. Your troops are armed with fifth-generation aircraft, precision-strike capabilities, advanced naval forces, and fully networked combat arms and land forces. From your command center you can precisely observe your forces on the battlefield, and your surveillance equipment allows unmitigated access to their actions and communications in real time. However, when you take this state-of-the-art force into combat against a near-peer competitor, nothing seems to work. Communications are at best intermittent and at worst nonexistent, your modern aircraft and naval assets cannot integrate operations, and your combat arms are relegated to utilizing line-of-sight communications to control the battle. The Clausewitzian "fog of war" settles on the joint operation, inducing confusion, ambiguity, and missed opportunities to advance the mission. At the tactical and operational levels of war, the ability to pass real-time decisions is gone, and the latency of information delays command decisions for 24 to 72 hours. The

Lieutenant Colonel Matthew J. Florenzen, USAF, is in the Central Security Service at the National Security Agency. Lieutenant Commander Kurt M. Shulkitas, USN, is the Military Advisor for Cyber and Information Operations at the Department of State. Major Kyle P. Bair, USA, is an Analyst in the Joint War Gaming and Experimentation Division at the Joint Staff J7.

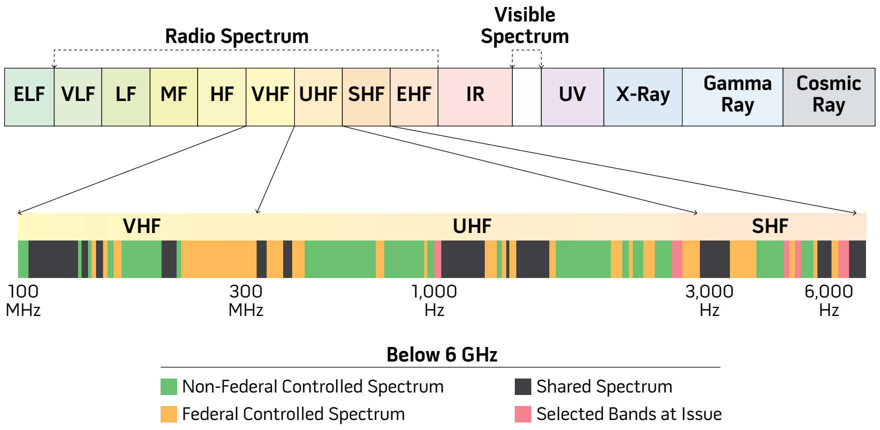
combined arms firepower of your joint force—the cornerstone of U.S. military doctrine—is combat-ineffective.

In this scenario, one potential issue complicating your operations might be an enemy exploiting your force's reliance on the electromagnetic spectrum (EMS). What do you see when you envision the EMS? It could be nothing that comes to mind, or maybe you picture the static joint doctrine description shown in figure 1. This article examines the benefits and risks associated with integrating artificial intelligence (AI) and machine learning (ML) technologies into the command and control (C2) systems guiding joint electromagnetic spectrum operations (JEMSO). To scope this discussion, this article examines how AI and ML solutions can improve a CCDR's ability to visualize, comprehend, and make informed decisions regarding the electromagnetic operating environment (EMOE).[1]

Figure 2 portrays how the U.S. Army perceives the EMOE. In today's information age, speed in the battlespace is predicated on information and the joint force's overall understanding of how the EMOE functions in joint operations. Understanding and visualizing the EMOE are crucial as military and civilian network interconnectedness and reliance on reliable access to the EMS increases. In turn, this interconnectedness and reliance help clarify the root problem: spectrum operations in today's information age and against a near-peer competitor pose significant regional and global challenges that will ultimately complicate a CCDR's ability to visualize and understand the EMOE with the required fidelity to make timely and appropriate JEMSO decisions. With this problem identified, this article examines the following question: can AI and ML improve a CCDR's understanding of a contested EMS, and what potential data quantity and quality pitfalls must be understood?

Three lines of effort are used to dissect this complex question. First, the article builds a common understanding of why AI and ML are being considered to improve CCDR EMS visualization. Second, it examines the potential roles for AI- and ML-enabled EMS visualization systems and provides a sample of what is currently available. Finally, it addresses the potential impacts of data types regarding AI and ML integration that must be considered in order to minimize risk. With this understanding of where we are currently, the capability of AI/ML to improve our EMS visualization and understanding, and clear appreciation for the role of data inputs to these systems, we gain a better appreciation of AI- and ML-enabled EMS visualization systems and how they might improve the decision cycle within the EMOE.

Figure 1. The Electromagnetic Spectrum



The top bar shows how the electromagnetic spectrum is divided into various regions and indicates that portion referred to as the radio spectrum. The lower bar illustrates the division of Federal, non-Federal, and shared bands for a critical part of the radio spectrum.

Legend

EHF: extremely high frequency
ELF: extremely low frequency
GHz: gigahertz
HF: high frequency
IR: infrared
LF: low frequency
MF: medium frequency
MHz: megahertz
SHF: super-high frequency
UHF: ultrahigh frequency
UV: ultraviolet
VHF: very high frequency
VLF: very low frequency

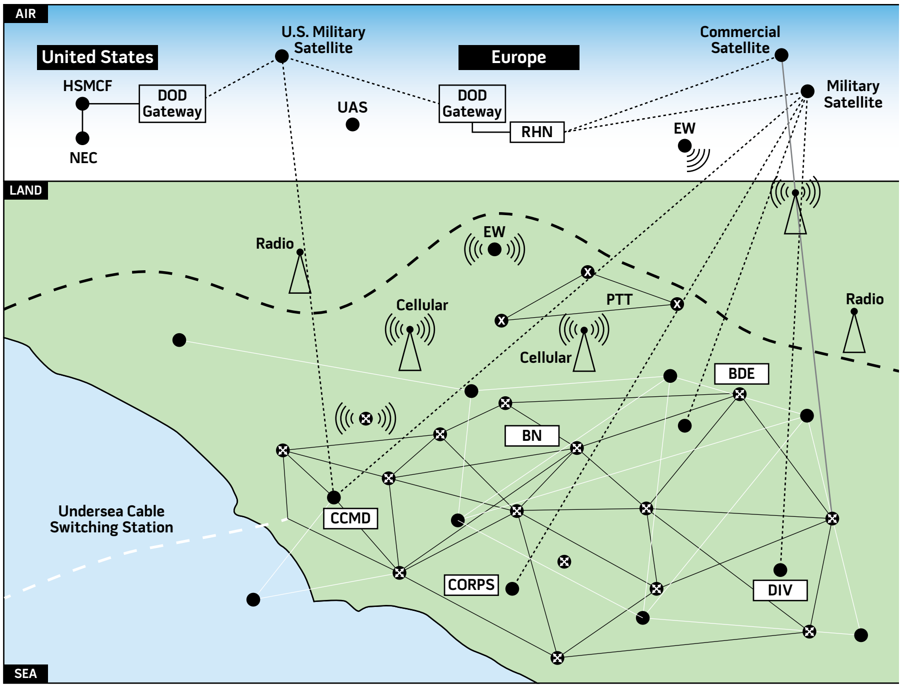
Impetus

Most of our modern military (and civilian) capabilities, warfighting systems, and businesses depend on open, trusted, and constant use of the EMS. Policies and procedures must lay the foundation for planning and mission preparation in a complex electromagnetic environment. The National Security Strategy, National Intelligence Strategy, and joint doctrine generally agree that near-peer competitors to Western ideals recognize the significant advantages provided by effective EMS operations. These important documents clearly indicate that developing and resourcing an electromagnetic capability to deter and defeat threats are imperative to U.S. national interests.

Ensuring constant and reliable access requires significant EMS connections to facilitate modern command, control, and communication linkages across military systems. The joint force attempts to achieve a credible means to maneuver within the EMS through joint electromagnetic spectrum management operations, which enable "EMS-dependent capabilities and systems to perform their functions in the intended environment without causing or suffering unacceptable interference."[2] While technical solutions are in development to meet this critical need, joint force spectrum management is largely accomplished manually through Excel spreadsheets and frequency listings. The manual processes used to manage the increasingly congested EMOE depicted in figure 3 are the antithesis of simplicity and should concern the warfighter.

To better manage this process, the joint force is developing JEMSO doctrine to guide the growing dependence on reliable EMS access. According to Joint Doctrine Note 3-16, *Joint Electromagnetic*

Figure 2. Visualization of Cyberspace and the Electromagnetic Spectrum in an Operational Environment



Legend

BDE: brigade
BN: battalion
CCMD: combatant command
DIV: division
DOD: Department of Defense
EW: electronic warfare
HSMCF: home station mission command facility
NEC: network enterprise center

PTT: push to talk
RHN: regional hub node
UAS: unmanned aerial system

- - International boundary
⊗ Network node
— Non-attributed network
····· Satellite transport

Source: U.S. Army Field Manual 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: Headquarters Department of the Army, April 2017), 1-3.

Spectrum Operations, "[JEMSO] are military actions undertaken by two or more Services operating in concert to exploit, attack, protect, and manage the EMOE. These actions include all joint force transmissions and receptions of electromagnetic (EM) energy."[3] The EMS is critical to the military's ability to execute operations and plays a similarly vital role in civilian infrastructures. The United States and its highly interconnected society are particularly exposed to a variety of EMS-related attacks, ranging from degraded communications and disrupted banking and financial transactions to interrupted electricity distribution. This dependency extends to U.S. military forces. In fact, the next armed conflict may be won or lost based on the fight for EMS superiority.[4]

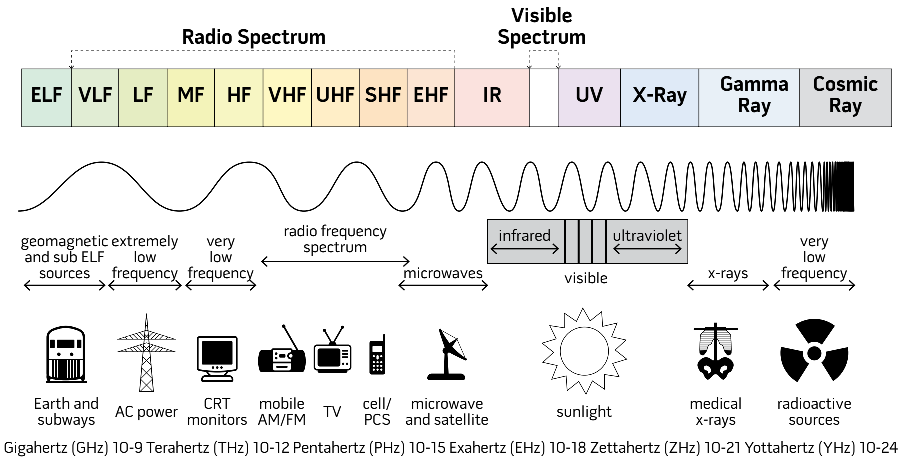
Adversaries are cognizant that effective EM measures during combat operations are vital to victory and may offset the military advantages enjoyed by the United States and its allies. The EMOE also provides an avenue for an adversary to influence the U.S. homeland in ways not possible during earlier conflicts. Near-peer competitors are incorporating progressive and innovative technologies that pose significant challenges to C2 and the infrastructures used in it.

The Defense Spectrum Organization (DSO) is the Department of Defense (DOD) Center of Excellence for spectrum management. DSO provides data-focused analytic expertise for military commanders, partners, and allies to enable spectrum management.[5] The analyses bolster the CCDR's ability to visualize and effectively employ operational capabilities within a complex electromagnetic environment. Comprehensively understanding the dynamic EMOE is vital for a CCDR to effectively shape and dominate the EMS and improve the capacity to identify, confront, circumvent, communicate, synchronize, and operate effectively.

The process employed to mitigate EMS fratricide is the joint restricted frequency list (JRFL), a "time and geographically oriented listing of . . . functions, nets, and frequencies."[6] However, the JRFL is still a list and does not readily improve a CCDR's ability to recognize EMS fratricide or visualize how the interference is affecting the battlefield. The current process to manage spectrum fratricide and interference is to file a report with the Joint Spectrum Interference Resolution (JSIR) program, which "identifies, reports, analyzes, and mitigates or resolves incidents of EMI [electromagnetic interference]."[7] Spectrum managers use the manual JSIR process to "report and diagnose the cause or source of all EMI (intentional/unintentional)."[8] The JSIR process quickly loses utility and effectiveness when facing a near-peer competitor attempting to affect the EMS in his favor or in a congested EMOE with constant EMI. In a contested or congested EMOE, friendly EMS fratricide and intentional interference by an enemy force are nearly indistinguishable.

With the 2019 JEMSO doctrine release, joint force commanders should expect improved integration of EMS operations. This doctrine reorganizes CCDR staffing functions and processes to recognize, report, and react to EMS interference sources; however, it does not singularly boost capacity or dramatically improve subject matter expertise running JEMSO cells. Humans have a limited ability to process the continually expanding amounts of EMS-related information in the EMOE. Additionally, humans manually processing the signal data lack the information quality required to visualize and understand the modern EMOE in battle-relevant time frames. The future of EMOE management hinges on system automation being able to inherently sense, display, and eventually modify friendly EMS-dependent systems operations to adapt to interference. Automated sensing and decisionmaking solutions must be employed to understand and visualize a complex EMOE and enable decisionmaking within the EMS that maximizes combat capability.

Figure 3. The Electromagnetic Spectrum



Legend

AC: alternating current
AM: amplitude modulation
CRT: cathode ray tube
EHF: extremely high frequency
ELF: extremely low frequency
EMF: electromagnetic field
FM: frequency modulation
HF: high frequency
IR: infrared
LF: low frequency
MF: medium frequency
PCS: personal communication system
SHF: super high frequency
TV: television
UHF: ultrahigh frequency
UV: ultraviolet
VHF: very high frequency
VLF: very low frequency

Current Initiatives

While the concepts and doctrine associated with JEMSO provide the joint force with necessary processes and a foundation for improving a CCDR's ability to see, understand, and make sense of the EMOE, the underlying technology is crucial to operationalizing the EMS as a warfighting capability. Even with the best trained personnel, processes, and plans, the future operating environment will be so complex that our ability to sense and orient the force to the EMS actions of a near-peer competitor will be virtually impossible. Numerous studies have determined that the character of war will continue to be increasingly reliant on the force's ability to sense and make sense of information. Workshops and war games repeatedly find that the ability to collect, process, and disseminate accurate battlefield intelligence to the right decisionmakers provides a key decisive edge.[9] To address this critical shortfall, DOD recognizes that the joint force must rapidly evolve in both its battlespace awareness and EMS agility to adequately compete in the next conflict. Legacy systems and engineering designs carried the force to where it is today, but the future promises known and unknown complex challenges that will test our ability to decisively act and react to changes in the competitive environment.

Before a discussion regarding active projects seeking to address the challenges faced in the EMS can commence, it is important to briefly discuss AI and ML. AI is an umbrella term used to describe a family of technologies and techniques seeking to allow machines to respond to external stimulation as humans might, with "contemplation, judgment, and intention."[10] Others take this idea one step further by broadly defining the qualities such systems and techniques must have. John Allen and Darrell West assert that AI systems should have "intentionality, intelligence, and adaptability."[11] As a recognized sub-discipline of AI, ML seeks to make sense of massive troves of data using computers that can react without running explicit rules-based programming functions. Essentially, the computers are deriving key relationships by learning from the data rather than being told what is important.[12] There are a variety of other ML techniques with a broad range of utility and effectiveness, but a deeper discussion of the full breadth and depth of AI and ML is beyond the scope of this article.

As the world continues to blur the boundary between possible and impossible with AI, DOD recognizes it must be at the forefront of the potentially disruptive technology. In June 2018, former Secretary of Defense James Mattis reorganized responsibility for DOD's AI initiatives from the Under Secretary of Defense for Research and Engineering, Michael Griffin, to DOD's Chief Information Officer, Dana Deasy, under a new organization, the Joint Artificial Intelligence Center (JAIC). The JAIC assumed coordination responsibilities for any AI-related project over $15 million, while the Services or sponsoring agencies maintain responsibilities for any project under $15 million.[13] Additionally, DOD released its 2018 AI strategy. The strategy, clearly informed by the other major national security strategies, broadly directs the Department to accelerate the adoption of AI while acknowledging that the technology will almost certainly change how DOD conducts business in potentially profound and unexpected ways.[14]

As DOD finally shines a spotlight on these disruptive and transformative technologies and acknowledges the need for coherent national AI strategies, research and development focused on utilizing AI and ML to improve how the United States leverages the EMS is increasingly important. One such project is the Defense Advanced Research Projects Agency (DARPA)–sponsored Radio Frequency Machine Learning System (RFMLS). RFMLS's goal is to "develop the foundations for applying modern data-driven machine learning to the RF [radio frequency] spectrum as well as to develop practical applications in emerging spectrum problems."[15] The effort sought to achieve four specific objectives. First, the system or system of systems should have the ability to learn features in order to directly use sensor data. Second, the system should be able to determine what EMS data are most important while

Marines from 2nd Radio Battalion, II Marine Expeditionary Force Information Group, and a Norwegian army electronic warfare operator employ Wolfhound Handheld Threat Warning System during Integrated Training Exercise 5-19 at Marine Corps Air Ground Combat Center, Twentynine Palms, California, July 30, 2019 (U.S. Marine Corps/Cedar Barnes)

simultaneously being able to recognize new signals of interest. Third, the system should be able to adaptively reconfigure sensors automatically to achieve optimum performance under given prevailing conditions. Finally, the system should have the capability to learn to synthesize and transmit entirely new engineering strong-motion ESM waveforms.[16] Another DARPA initiative is the Adaptive Radar Countermeasures (ARC) program. This program seeks to leverage ML and advanced signal processing to dynamically characterize a potential radar threat, even one never observed; synthesize a countermeasure (for example, conduct jamming); and then evaluate the countermeasure's battlefield effectiveness.[17]

Thanks to programs like RFMLS and ARC, the pace of EMS operations and our reliance on them will only increase. Near-peer competitors will attempt to exploit joint force EMS dependency, seeking to isolate systems specifically designed to use the EMS to optimize and integrate warfighting functions. The complexity of the environment requires that today's CCDR can understand, visualize, and act within the EMS to fully employ the broad capabilities of their fighting forces.

This is where the utility of AI- and ML-enabled EMS visualization systems can truly impact the total force operations by recognizing and reacting to a fluid EMOE. By integrating systems that can communicate among themselves without operator intervention and can incorporate the necessary bits of information that otherwise would be background noise to the human operator, improvements can be made in the ability to sense EMS actors and emissions. By applying a variety of models, AI- and ML-assisted systems can begin to categorize individual emissions and their impacts to friendly force EMS operations. With that said, the ability of AI and ML systems to access, process, and report on the EMS poses some operational challenges.

The Future Need

Incorporating AI into the EMOE visualization and understanding process will support the growing speed of JEMSO; however, AI, ML, and deep learning models depend on reliable and trusted data to ensure learning is not corrupted. The dependence on data in both quality and quantity poses the greatest risk to integration of AI and ML technologies into the JEMSO processes. In June 2015, the U.S. Army Research Laboratory conducted a workshop to visualize the tactical ground battlefield in 2050 and reported that "the roles of information technologies will co-evolve (that is, will influence and be influenced by) future concepts and technologies for key warfighting functions, including seeing (sensing), understanding, communicating . . . capabilities that are involved in obtaining, collecting, organizing, fusing, storing, and distributing relevant information as well as the capabilities associated with C2 functions and processes including reasoning, inference, planning, decisionmaking."[18]

Up to this point this article has discussed the current limitations in sensing and understanding the EMOE and the role of AI and ML technologies and how they can change the tools available to accomplish these tasks. In order to realize the potential advantages offered by introducing AI and ML capabilities into our JEMSO C2 systems, there must be clarification of the basic requirements for sensing, visualizing, and informing decisions regarding the EMS.

First, sensing is the process of collecting, routing, and storing information that will form the building blocks for further analysis and processing. Using EMS sensors to facilitate this is not a new concept. Nearly every fielded system in the military today has an aperture designed to facilitate its own limited EMS sensing requirements. So how does application of AI and ML change the role of these apertures to enable enhanced and centralized EMS sensing? More specifically, what level of EMS sensing is required to facilitate a CCDR's decisionmaking regarding JEMSO? The answer is not in the apertures; instead, it lies in how one connects and moves the information to a central processing system enabled by AI and ML. This information or data is working through the AI and ML models to provide the learning context for these systems, which builds understandable visualization, improves them over time, and ultimately allows a CCDR to understand where, how, and to what effect all EMS actions are having on the EMOE.

Imagine the EMOE as an ecosystem. Within it, the AI and ML would represent a central nervous system, connecting the individual sensor neurons and processing inputs from them to understand the environment. In this same ecosystem, the data from these sensors could be represented by the blood that fuels the decisionmaking and learning models for the AI and ML systems. Today, each individual aperture is isolated, reporting only to its own internal and limited system for a designed function related to the same individual system. By integrating AI and ML processes into our JEMSO systems, we can connect these apertures, or more accurately the data they are sensing becomes connected, to a central nervous system capable of moving and storing the information meeting multiple EMS purposes simultaneously. This idea is commonly referred to as the "big data" concept.[19] In the simplest terms and for the scope of this article, two types of data concepts are examined, "big" data and "deep" data. Arguments can be made on the advantages and disadvantages of these data sets. In truth, battlefield commanders will require both.

Let us begin by clarifying in simple terms the differences between big and deep data sets. The working definition of *data* for our discussion is bits of information that can be combined to depict a pattern of information that can be used to visualize the EMS. In this simple definition, an individual data point is not of much value to improving AI and ML technologies or recreating near real-time EMS visualization. To do this, automated systems will require multiple data sets or groupings of these individual data points that, when combined, begin to tell a story about the nature of the EMOE. Common approaches for collecting these data sets are where the terms *big* and *deep* enter the discussion. For the purpose of this article, *big data* is used to reference the collection of massive quantities of data sets from across a wide set of sensors. The advantage of big data in this definition is in its ability to scrape a vast quantity of data points from the EMOE for any snapshot in time. It does this by integrating and pulling shallow data sets from multiple sensors for a defined time slice and providing these individual data points to the AI ecosystem. The AI/ML system can rapidly compare these snapshots, using them to recognize patterns occurring in the environment.

While the idea of having thousands of EMS sensors each providing inputs from their individual apertures' perspective into a visualization system may initially sound like an easy answer, the issue is more complex. Moreover, commanders make decisions not on data but rather on intelligence, and "it is the job of the Intelligence Community to analyze, connect, apply context, infer meaning, and ultimately make analytical and operational judgments based on all available data."[20] Since data in its rawest form builds the individual pixels of information to be used by AI/ML systems to learn, the sources and quality must be controlled to reduce risk and prevent unwanted manipulation. Failure to ensure the quality of data sets can change the processing and dissemination of the intelligence being produced. Conversely, *deep data* sets are used to describe the detailed quality of an individual data point against a singular purpose or target over time to build behavioral relationships and to add depth of understanding.[21] Through deep or analyzed data, EMS visualization takes on context and meaning. By combining both deep and big data sets into our ML and deep learning models, EMS visualization systems can rapidly sense the EMOE and focus intelligence analysis efforts against it to enable meaningful understanding. In other words, if big data provides the *what*, then deep data provides the *so what*. With both the what and the so what bits of information, intelligence processes can be streamlined, resulting in actionable EMS visualization and understanding informing the CCDR decision processes. Therefore, while the idea of big data does offer a capability to rapidly sense the EMOE, it must be measured and weighed against deep data sets to reduce the risks of data corruption and to provide the intelligence necessary to understand the EMOE.

Next is communicating this information in a way that enables a commander and staff to quickly understand it, enabling them to make informed decisions on JEMSO. Today, our forces employ many variations of EMS modeling capabilities to help them build graphical understanding and visualization of the EMS—everything from 3D modeling to waterfall spectrum charts and maps with specific emitter graphics and details. However, all of these visualization tools are costly in time and labor and do not have the capacity to work with the vast amount of data available through an AI-enabled EMS sensing solution. To reduce the processing time required and accurately relay the EMOE

Marine with electronic warfare liaison element, Marine Rotational Force–Europe 19.2, Marine Forces Europe and Africa, prepares for tactical extract during exercise Valhalla in Setermoen, Norway, June 17, 2019 (U.S. Marine Corps/Larisa Chavez)

at the speed of battle, these modeling tools must leverage or become a function of the same AI learning systems used to collect and process the EMS data/information. To simplify, the same AI and ML technology that is integrating the EMS abilities to sense, visualize, and understand can simultaneously direct refined intelligence analysis and graphical modeling programs. Not only can it do this, but it also should do this to provide CCDRs a visual depiction of what is being detected in the EMS, relationships and behaviors tied to the detections, and how their forces are responding. Admittedly, this may present some risk by prematurely acting on information before detailed intelligence analysis is accomplished. To mitigate this risk, human expertise is required in the processes.

The human expertise residing in the JEMSO planning and execution cells will serve to coordinate these actions, but the design of the visualization must be simplified to allow for immediate and detailed understanding. To put this in context, today within most of the land, maritime, air, or space operations centers, a CCDR can look up to the big screens and quickly see and understand where forces are and what actions are being performed. However, there is not visualization of what the EMS looks like around them or what is being done within it to ensure they are connected to the rest of the force. In a limited engagement, we can get away with this lack of understanding and visualization, but against a near-peer competitor we will quickly see our forces isolated from the rest of the military systems supporting them if we fail to visualize and understand the EMOE.

Conclusion

Let us again imagine you are a CCDR equipped with the very best capabilities today's military can offer. But now add into your tool kit a C2 system that incorporates emerging JEMSO doctrine and is enabled by AI and ML technologies. These technologies rapidly connect the thousands of apertures across the battlefield and report back to command systems, providing both big and deep data sets—data sets that can be applied to the AI and ML systems to increase system learning of the EMOE in detail. Armed with these systems and your network of data providers, you can rapidly detect, report, and produce visualization tools that allow you to understand the changes in your EMOE as they are reported, enabling you to make effective and timely decisions to protect and ensure your force access to the EMS. Given this system, the CCDR sees and understands the EMOE, quickly recognizing and mitigating near-peer competitors' attempts to affect friendly force spectrum assurance. Having gained an increased understanding of the EMOE, the CCDR can mitigate EMS impacts and maximize the joint force's warfighting potential.

By integrating AI and ML systems into the JEMSO C2 doctrine and processes, a CCDR is better equipped to visualize and understand his EMOE at the speed of battle in the information age. The need for improved processes to sense and make sense of the EMS and how it is intertwined within our military and national networks has been identified as critically important by all levels of our strategic guidance, yet DOD has no solutions currently fielded to address the issues. By incorporating smart and automated systems that apply a variety of learning models, we can improve the EMS visualization processes and better understand the nature of the information fueling these systems. The Defense Department can reduce the risks associated with capacity saturation by balancing between deep and big data solutions that enable us to understand and visualize the EMOE. The safety and combat effectiveness of the joint fighting force demand AI solutions that preserve the capacity to sense and make sense of an incredibly complex electromagnetic operating environment. Now is the time to lift the electromagnetic fog of war. **JFQ**

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 1-0, *Personnel Support*

JP 2-0, *Joint Intelligence*

JP 3-05, *Special Operations*

JP 3-26, *Combating Terrorism*

JP 3-40, *Countering WMD*

JP 5-0, *Joint Planning*

JP 6-0, *Joint Communications System*

JPs Revised (signed within last 6 months)

JP 1, *Doctrine for the Armed Forces of the United States*, vol. 1

JP 3-09, *Joint Fire Support*

JP 3-09.3, *Close Air Support*

JP 3-10, *Joint Security Operations*

JP 3-29, *Foreign Humanitarian Assistance*

JP 3-30, *Joint Air Operations*

JP 3-31, *Joint Land Operations*

JP 4-09, *Distribution Operations*

JP 4-10, *Operational Contract Support*

Notes

[1] The *electromagnetic operating environment* (EMOE) is defined as "the background [electromagnetic] radiation and the friendly, neutral, and adversarial electromagnetic [activity] within the [electromagnetic area of influence] associated with a given operational area." See Chairman of the Joint Chiefs of Staff Memorandum 3320.01C, *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment* (Washington, DC: The Joint Staff, December 14, 2012), appendix D to enclosure C, C-D,1. The EMOE is a complex composite of the electromagnetic conditions, circumstances, and influences that affect the employment of capabilities and the decisions of the commander.

[2] Joint Publication 6-01, *Joint Electromagnetic Spectrum Management Operations* (Washington, DC: The Joint Staff, March 20, 2012), viii.

[3] Joint Doctrine Note (JDN) 3-16, *Joint Electromagnetic Spectrum Operations* (Washington, DC: The Joint Staff, October 20, 2016), I-1.

[4] Ibid., v.

[5] See Defense Information Systems Agency, "About DSO" [Defense Spectrum Organization], available at <https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/about-dso>.

[6] JDN 3-16, C-1.

[7] Ibid., I-9.

[8] Ibid.

[9] Alexander Kott et al., *Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report*, ARL-SR-0327 (Adelphi, MD: U.S. Army Research Laboratory, June 2015), 22.

[10] Shukla Shubhendu and Jaiswal Vijay, "Applicability of Artificial Intelligence in Different Fields of Life," *International Journal of Scientific Engineering and Research* 1, no. 1 (September 2013), available at <https://pdfs.semanticscholar.org/2480/a71ef5e5a2b-1f4a9217a0432c0c974c6c28c.pdf>.

[11] Darrell M. West and John R. Allen, *How Artificial Intelligence Is Transforming the World* (Washington, DC: The Brookings Institution, April 24, 2018), available at <www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/>.

[12] Daniel Faggella, "What Is Machine Learning?" *Emerj*, February 19, 2019, available at <https://emerj.com/ai-glossary-terms/what-is-machine-learning/>.

[13] Sydney J. Freedberg, Jr., "Joint Artificial Intelligence Center Created Under DOD CIO," *Breaking Defense*, June 29, 2018, available at <https://breakingdefense.com/2018/06/joint-artificial-intelligence-center-created-under-dod-cio/>.

[14] *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington, DC: Department of Defense, 2018), available at <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/summary-of-dod-ai-strategy.pdf>.

[15] Radio Frequency Machine Learning Systems program, Defense Advanced Research Projects Agency–funded program solicitation, Duke University Web site, 2017, available at <https://researchfunding.duke.edu/radio-frequency-machine-learning-systems-rfmls>.

[16] Ibid.

[17] Adaptive Radar Countermeasures, BAE Systems Web site, 2017, available at <www.baesystems.com/en-us/product/adaptive-radar-countermeasures-arc>.

[18] Kott et al., *Visualizing the Tactical Ground Battlefield in the Year 2050*, I-2.

[19] This reflects the authors' generalized definition of *big data* as applied to the context of this article only.

[20] *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, DC: Director of National Intelligence, December 2018), 1, available at <www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf>.

[21] This reflects the authors' generalized definition of *deep data* as applied to the context of this article only.

CALL FOR ENTRIES

for the

2020 Secretary of Defense and
2020 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. These rewards, along with a monetary prize, await the winners.

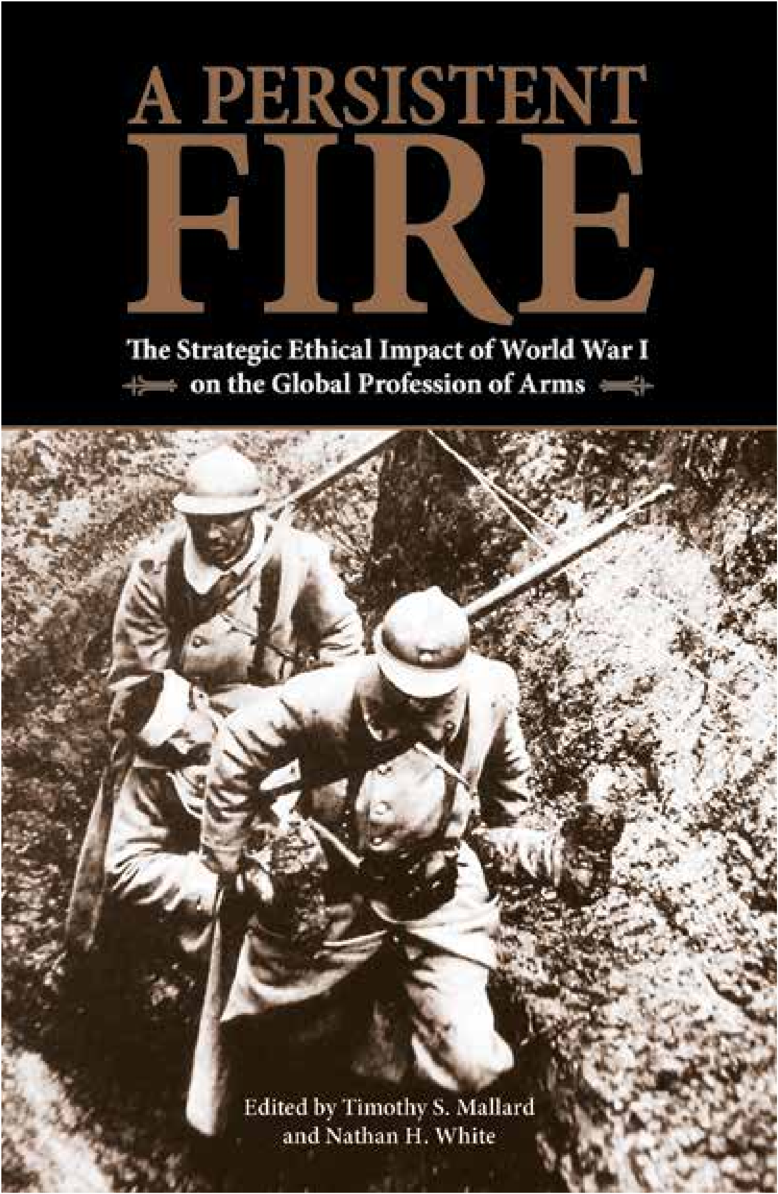
Who's Eligible? Students, including international students, at U.S. PME colleges, schools, and other programs, and Service research fellows.

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 2019–2020 academic year. Students are encouraged to begin early and avoid the spring rush. Final judging and selection of winners take place May 2020, at NDU Press, Fort McNair, Washington, DC.

For further information, see your college's essay coordinator or go to:

http://ndupress.ndu.edu/About/Essay-Competitions/


A PERSISTENT FIRE
The Strategic Ethical Impact of World War I on the Global Profession of Arms
Edited by Timothy S. Mallard and Nathan H. White

New from NDU Press

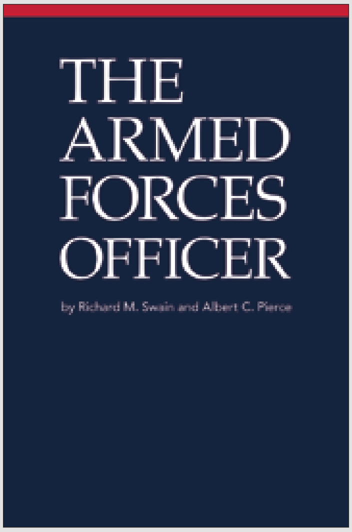
A Persistent Fire: The Strategic Ethical Impact of World War I on the Global Profession of Arms

Edited by Timothy S. Mallard and Nathan H. White
2019 • 412 pp.

Since "the war to end all wars" witnessed the rise of global war among competing nation-states conducted in often tenuous alliances with nascent professional militaries—characteristics that continue to mark contemporary warfare a century later—then studying that conflict's impact seems a relevant method to decide ways in which the profession of arms will develop in the next 25 to 50 years. Indeed, like a smoldering, persistent fire that threatens to re-erupt into a fresh conflagration, World War I continues to deeply shape and guide the profession of arms today.

Download the EPUB, MOBI, or PDF version for free.

Scan the QR Code above or go to:
http://ndupress.ndu.edu/Publications/Books/A-Persistent-Fire



THE ARMED FORCES OFFICER

by Richard M. Swain and Albert C. Pierce

From NDU Press

The Armed Forces Officer

2017 • 212 pp.

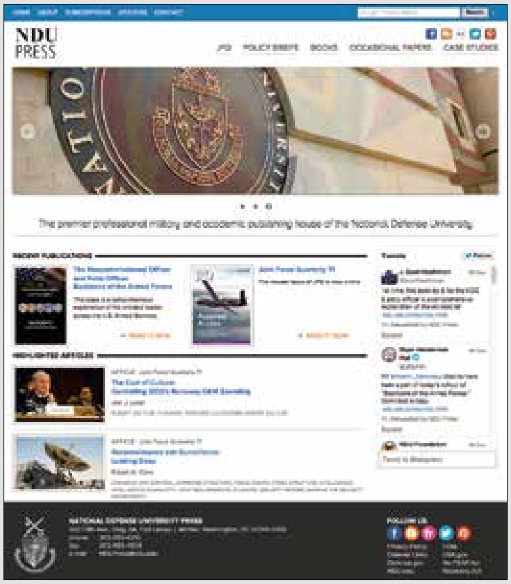
From the Foreword by General Joseph F. Dunford, Jr.:

"In 1950, the great Soldier-Statesman George C. Marshall, then serving as the Secretary of Defense, signed a cover page for a new book titled *The Armed Forces Officer*. That original version of this book was written by none other than S.L.A. Marshall, who later explained that Secretary Marshall had 'inspired the undertaking due to his personal conviction that American military officers, of whatever service, should share common ground ethically and morally.' Written at the dawn of the nuclear age and the emergence of the Cold War, it addressed an officer corps tasked with developing a strategy of nuclear deterrence, facing unprecedented deployments, and adapting to the creation of the Department of Defense and other new organizations necessary to manage the threats of a new global order.

"This new edition of *The Armed Forces Officer* articulates the ethical and moral underpinnings at the core of our profession. The special trust and confidence placed in us by the Nation we protect is built upon this foundation. I commend members of our officer corps to embrace the principles of this important book and practice them daily in the performance of your duties. More importantly, I expect you to imbue these values in the next generation of leaders."

Available at ndupress.ndu.edu/Media/News/Article/1159223/the-armed-forces-officer/

Have you checked out NDU Press online lately?



NDU PRESS

JFQ POLICY BRIEFS BOOKS OCCASIONAL PAPERS CASE STUDIES

The premier professional military and academic publishing house of the National Defense University

With 20,000 unique visitors each month, the NDU Press Web site is a great place to find information on new and upcoming articles, occasional papers, books, and other publications.

You can also find us on:

Facebook

Flickr

Twitter

Pinterest

Visit us online at: **https://ndupress.ndu.edu**

JFQ

JOINT FORCE QUARTERLY

Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

NDU Press