National Defense University

Digital Commons @ NDU

10-2020

Joint Force Quarterly 99 (4th Quarter, October 2020)

National Defense University Press

JFQ | Joint Force Quarterly

Issue 99, 4th Quarter 2020

Social Media Weaponization

A Brief History of the Insurrection Act

2020 Essay Competition Winners

Cover 2 images (top to bottom): Lance Corporal Joshua Anderson, rifleman with 3rd Battalion, 4th Marine Regiment, 1st Marine Division, relays commands to his fire team while conducting offensive operations during Supersquad 2020 Competition at Marine Corps Base Camp Pendleton, California, August 20, 2020 (U.S. Marine Corps/Kyle C. Talbot); Explosive Ordnance Disposal 2nd Class Travis Lamson and his team, assigned to Explosive Ordnance Disposal Mobile Unit 2, conduct gear check while on standby in SH-60F Sea Hawk helicopter assigned to Nightdippers of Helicopter Anti-Submarine Squadron 5, September 8, 2012 (U.S. Navy/Ryan D. McLearnon); Sailor in firefight ensemble after combating fire aboard amphibious assault ship USS *Bonhomme Richard*, moored pier side at Naval Base San Diego, July 15, 2020 (U.S. Navy/Julio Rivera)

In This Issue

About the Cover

Private First Class Courtney Gibson, assigned to 554th Military Police Company, provides security from Humvee gunner's turret during training exercise in Boeblingen, Germany, February 10, 2015 (U.S. Army/Martin Greeson)

President Lyndon B. Johnson hands pen to Senator Robert F. Kennedy during signing ceremony for Voting Rights Act, U.S. Capitol, Washington, DC, August 6, 1965 (White House Photo Office/LBJ Library/Robert Knudsen)

Executive Summary

In an address in Cape Town, South Africa, on June 6, 1966, Senator Robert F. Kennedy stated, "There is a Chinese curse which says, 'May he live in interesting times.' Like it or not, we live in interesting times. They are times of danger and uncertainty; but they are also the most creative of any time in the history of mankind." As it turns out, we ourselves are living in interesting times: from the worldwide COVID-19 pandemic to racial strife, wildfires to record numbers of hurricanes, contested politics to economic crises, and more.

But when we take a hard look and do some digging, we find that while we as individuals may not have been in such circumstances, others have and found ways to "soldier on." Otherwise, the human race would have long ago ceased to exist. This indomitable spirit is exactly what jointness does for the American military: it provides the ways and means to continue to survive and provide, collectively, for the defense of our nation. Left to figure out how to defend the United States alone,

the individual Services would likely find themselves in even more interesting times.

The early battles over aerial bombing of naval ships, the "Revolt of the Admirals," dividing up airpower in Vietnam, the *Mayaguez* incident, Operation *Desert One*, Grenada, and more all point to the need for more jointness, not less. We have learned that we can accomplish more when we work together to secure the Nation, especially when readiness is low and resources are overstretched. "Teamwork makes the dream work," my wife often says. How could it be otherwise? Sometimes we need to be reminded of how much we rely on each other. Often it is as simple as rereading our nation's foundational documents and trying to understand what they mean and how we should best defend what they stand for.

Our Forum presents four important articles that take us from the battlefield in a traditional sense to the far reaches of the newest domain of cyber. First, Sarah Gamberini helps us explore the potential effects of Russian disinformation

campaigns (yes, they do exist) through the medium of social media and their impact on public health. Still much a concern related to our battles in cyberspace, Jesse Samluk, Mark Boeke, and Marcus Neal provide a solid set of criteria for updating how the Services might recruit future cyber warriors. While no one would question the strategic importance of space, Jerry Drew helps us explore the operational and tactical issues all of us need to understand as we consider space operations and the potential for warfighting in space. Back here on Earth, Michael Fenzel, assisted by Leslie Slootmaker and Kim Cragin, discuss lessons learned on how to develop strategic insights from exploitable material collected from the battlefield.

Successful virtual Secretary of Defense and Chairman of the Joint Chiefs essay competitions were held earlier this year, and NDU Press proudly presents the winners of some very close contests. So close, in fact, that we declared a tie in the Secretary of Defense Strategic Research Paper category. From the

U.S. Army War College, Roderick Butz offers his research on the use of remotely piloted airstrikes as a tool of statecraft. Answering the call for ideas about Great Power competition with China, Kaleb Redden, from the National War College, offers his suggested U.S. strategy toward the People's Republic of China. Jeremy McKissack, from the Air War College, won the Chairman of the Joint Chief's Strategy Paper category with his analysis of President Donald Trump's interventions in military justice cases. In the Chairman's Strategy Article category, Mark Zais, of the U.S. Army War College, gives us his take on artificial intelligence and military decisionmaking. Due to circumstances beyond our control, we are unable to provide Roderick Butz's winning essay in this issue but will do so as soon as possible.

In Commentary, we get an expert practitioner's view as Terrence O'Shaughnessy helps us understand how we can leverage the emerging Joint All Domain Command and Control to achieve decision superiority. From the chaplain to the Chairman of the Joint Chiefs of Staff, Wayne Macrae discusses how to understand religion in relation to the joint force. Part of his work is in assisting the development of new joint doctrine in this area. As leaders at all levels grapple with the added load of working during a global pandemic, Russell Williford and Wendi Peck offer their suggestions on how to achieve success in military organizations.

Leading off Features, James Cook offers an excellent article on the value of joint concepts to a joint planner. After several calls from my colleagues here at the Eisenhower School for more articles on mobilization, and having a second place winner in the 2019 Chairman of the Joint Chiefs of Staff Strategy Paper competition at hand on the topic, we offer Matthew Gaetke's views on the right questions to ask as we consider what mobilizing for war today should resemble. Next, Michael St. Jeanos offers an up-to-date primer on the U.S. Coast Guard. And to help us understand the connections between the "boom" and the "zaps," Josiah Dykstra, Chris Inglis, and Thomas Walcott describe

Attorney General Robert F. Kennedy speaks to crowd about racial equality, outside Justice Department, June 14, 1963 (Library of Congress)

how to integrate physical and cyber weapons in combat.

In Recall, we are pleased to offer two fine articles that tie us to our past in order to understand what we could and should do in the future. From the Joint Staff History Office, Michael Rouland and Christian Fearer help us learn about the long and nuanced history of the Insurrection Act. The first lesson is that there is no such act. Most military history students look to World War II for lessons of fighting with allies, but Fideleon Damian offers an excellent account of coalition operations in the opening year of the Korean War. In addition, we bring you three excellent book reviews and our joint doctrine update.

Robert Kennedy's speech that day in 1966—on a then unprecedented trip and exactly 2 years before his assassination—included some words that may help all of us see our road ahead a bit more clearly. He stated, "It is from numberless diverse acts of courage such as these that the belief that human history is thus shaped. Each time a man stands up for an ideal, or acts to improve the lot of others, or strikes out against injustice, he sends forth a tiny ripple of hope, and crossing each other from a million different centers of energy and daring those ripples build a current which can sweep down the mightiest walls of oppression and resistance." To me that is what Americans, especially those in uniform, aspire to do. Let us know what you think. Be safe. **JFQ**

William T. Eliason
Editor in Chief

Senior Airman Marcel Williams, 27th Special Operations Wing public affairs broadcaster, speaks at "Gathering for Unity" event at Cannon Air Force Base, New Mexico, June 5, 2020, and shares experiencing racism in his own community (U.S. Air Force/Lane T. Plummer)
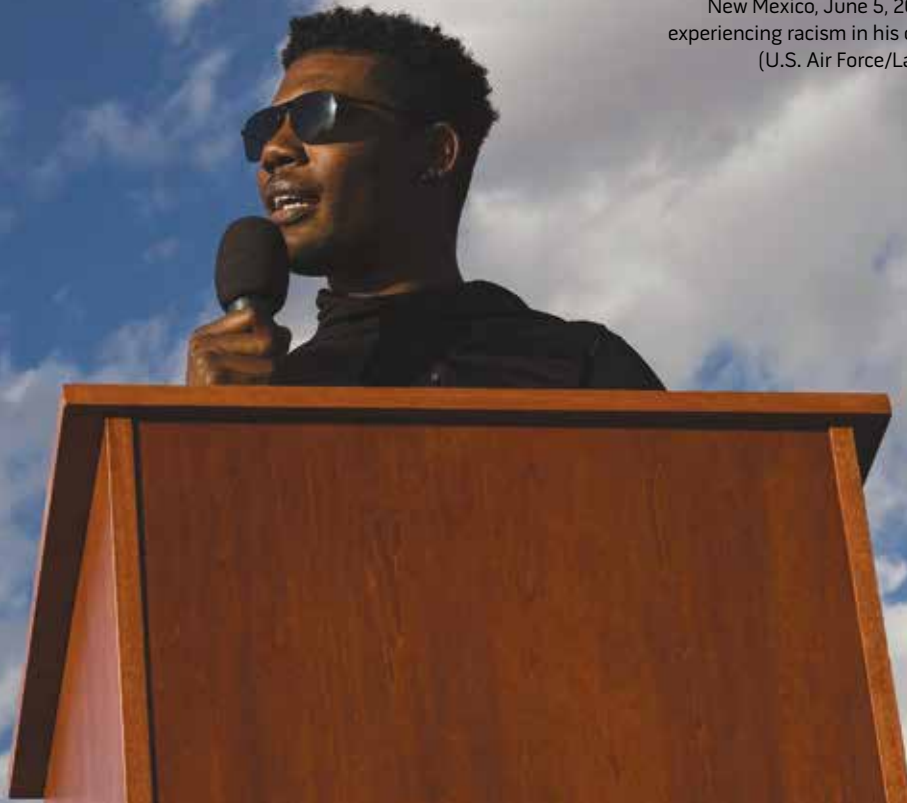
Social Media Weaponization
The Biohazard of Russian Disinformation Campaigns

By Sarah Jacobs Gamberini

Sarah Jacobs Gamberini is a Policy Fellow in the Center for the Study of Weapons of Mass Destruction, Institute for National Strategic Studies, at the National Defense University.

In a renewed era of Great Power competition, the United States is faced with adversaries engaging across multiple domains without the traditional distinctions of war and peace. America's competitors are regularly operating below the threshold that would warrant a military response, including on the information battlefield. The blurred red lines that result from covert information operations waged by foreign actors on the Internet will force a change in how the United States operates and how its society consumes information. Russia used tactics of influence and coercion long before social media allowed for nearly ubiquitous access to its targets and a prolific capability for controlling a narrative and manipulating the hearts and minds of a population on a range of sensitive societal issues, including public health.

Russia has a long history of seeking to project power and influence while playing with a technological and geopolitical handicap. Given its history and a geographic location with many bordering

nations, it sees itself as constantly besieged from all sides, but particularly by the West. Since the nadir of Soviet dissolution, Russia has fought to rebalance power and contemporaneously reduce American influence. But without equivalent conventional military might, Russia has turned to other asymmetric advantages to compensate in its competition with the United States. Social media has provided a unique tool kit to manipulate narratives and amplify societal divisions in an effort to weaken the United States in ways previously unimaginable. While Russian weaponization of information is not new the intersection of Russian disinformation, public health crises, and vulnerability to bioevents presents new and troubling homeland and national security threats for the United States.

The United States is diverse, pluralistic, and democratic. These characteristics, its founding principles, are also its strengths as a nation. But to U.S. adversaries, including Russia, they are potential weaknesses to exploit. One strategic goal of Russia's influence operations is to weaken the United States and its allies, which Russia views as operating too close to its sphere of influence, what it refers to as its "near abroad."[1] Time and again, Russia has used familiar influence tactics to spread disinformation in an attempt to weaken U.S. democratic society and defame America's reputation on the world stage.[2] From Russia's interference in the 2016 Presidential election to spreading hoaxes during the 2020 global pandemic, Russia is exploiting America's divisions with disinformation to amplify discord in the United States and undermine its institutions. As Russia targets issues of public health in this way, there will be tremendous implications for American citizens and the U.S. health system. The world is grappling with an "infodemic" as well as a pandemic, and both require a whole-of-society approach to be successfully addressed.[3]

Russia Under Siege

Over centuries, Russia has experienced attacks from the Teutonic Knights, Napoleon, and Nazi Germany, and, since the end of the Cold War,

encroachment from the United States and the North Atlantic Treaty Organization (NATO). It views the United States, NATO, and the European Union as committed to weakening Russia, eliminating its sphere of influence, and ensuring sustained U.S.-Western unipolar dominance.[4] This assessment derives from a strong Russian belief that the United States broke its word that NATO would move "not one inch eastward," as stated by then–U.S. Secretary of State James Baker in the aftermath of the Soviet dissolution.[5] Russia touts the West's "interference" during the Ukrainian revolution as further evidence that the United States and NATO are meddling too much in its area of influence.[6] It views this infringement on what it perceives as its near abroad as an unacceptable affront.[7]

Russia sees Western dominance manifested socially and culturally (for example, Western entertainment seeking to replace Russian culture, values, and language), politically (the West fomenting "color revolutions" in Russia and the former Soviet Union), and militarily (the United States geographically encircling Russia with NATO expansion and technologically ringing Russia with missile defenses and bases). Moreover, Russia has long feared it is behind the West in science and technology. Russia has, at times, achieved parity in certain defense platforms but generally struggles to keep pace, thus relying heavily on traditional weapons of mass destruction, such as its substantial nuclear arsenal, to offset U.S. conventional might. Russia similarly lags in technologies for civilian applications. Underlying all this are vast and troubling demographic and health challenges (a declining birth rate and high death rate from unnatural causes, including widespread alcoholism).[8] These factors have led to Russia viewing itself in a constant state of besiegement and deficiency.

Much of what shapes and propels Russia's worldview today is based on former Prime Minister Yevgeny Primakov's doctrine that rejects the United States as a hegemon and seeks a multipolar world and the reestablishment of Russia as the main regional power in the former Soviet

region.[9] Since the end of the Cold War, Russia has had to be calculating and creative to balance its economic, military, and technological disadvantages to compete with the United States, maximizing less conventional tools of war, including covert operations within the information domain.

During the Cold War, the Soviet Union used active measures to influence nations in coercive ways distinct from espionage and counterintelligence. Active measures included disinformation, political influence operations, and controlling media and messaging with the goal of discrediting or influencing the West, which are echoed in Russia's modern-day tactics.[10] This type of warfare and other measures below the threshold of actual use of force have been variously referred to in the West as Russia's *asymmetric*, *gray zone*, *hybrid*, or *next-generation warfare*. However, the term *cross-domain warfare* better reflects the current Russian method of shaping the security environment using an integrated approach of all military and nonmilitary devices to achieve its strategic goals.[11]

In a response to the Arab Spring uprisings, which Russia believed to be incited by the West, General Valery Gerasimov (now chief of the General Staff) publicly discussed how to prevent similar uprisings in Russia. In his speech, Gerasimov cited control of information as central to victory.[12] This speech, which has been overstated as a Russian military doctrine, did describe how Russia should operate simultaneously across multiple domains—military, political, cyber, and information warfare—to achieve strategic goals. In March 2019, Gerasimov spoke on the shift of warfare to the information sphere and labeled information technologies as "one of the most promising types of weapons" to be used covertly "not only against critically important informational infrastructures, but also against the population of a country, directly influencing the condition of a state's national security."[13]

Information is but one aspect of cross-domain warfare. Another important facet of this Russian thinking is the belief that the customary distinction between

Control room operators with Edgewood Chemical Biological Center aboard U.S. Government–owned container ship MV *Cape Ray*, modified and deployed to eastern Mediterranean Sea to dispose of Syrian chemical agents, confirm and record data on current operation at Naval Station Rota, Spain, June 16, 2014 (U.S. Navy/Desmond Parks)

wartime and peacetime no longer exists. These blurred red lines have been demonstrated beyond speeches or doctrine, for instance in Russia's employment of this malign activity below the U.S. threshold of armed conflict—little green men in Crimea and Eastern Ukraine, "unaffiliated" private military groups in Syria, use of Novichok (a Cold War–era chemical weapon first developed by the Soviet Union) in the United Kingdom, and numerous cyber attacks—and by the nature of cloaked activities, likely many more. Yet Russia has protected itself from military response because attribution and proportionality are thrown into question by their deniability and obfuscation.

Old Influence Operations Playbook, New Media Tools

Russia's present leaders fear that U.S. advantages in information technology allow Washington and its allies to undermine Russian social, cultural, and political institutions as part of its broader campaign to ensure Western geopolitical dominance.[14] The Kremlin sees information as a new type of weapon and views all forms of information, across all platforms, as potential sources of power to be weaponized. Russia believes that the West is using all forms of information technology against them—from persistent satellite television and the Internet bombarding Russian citizens with what it views as overtly anti-Russian messages to social media as tools for coordinating activists and provocateurs in uprisings in former Soviet republics. Finally, Russia sees U.S. space, intelligence, surveillance, and reconnaissance, as well as other information technology systems, as networked military capabilities designed to summarily dismantle any opponent slow to adapt.

Russia has responded to this threat of the information age in a number of ways. It is working to create a "Russia only" Internet with aspirations of creating a Russian equivalent of China's "Great Firewall."[15] Russian news and propaganda (for example, the state-controlled television network RT and online "news" aggregators such as Sputnik) are beamed in to counter Western cable news.[16] Additionally, until Russia has its own information operations military systems, it holds Western systems at risk both physically (for example, antispace capabilities) and with cyber attacks.[17] Finally, the Russian government's active Internet presence pervades the social media landscape using large numbers of Russian Web brigades, troll farms, and automated bots to disseminate propaganda and flood hashtags.[18]

Coinciding with its view that all information can be leveraged, Russia's social

media machine is employed to great effect to influence its adversaries and their populations. Russian trolls utilize the power of narratives online, focusing on simple messages targeting a cohesive group so that its message will then be shared and further amplified by foreign targets.[19] They have a keen understanding that strong emotions spread quickly online and that, given the right prompting, people love nothing more than arguing and solidifying entrenched viewpoints.[20] As with Soviet active measures, Russia's goals in weaponizing social media are to foment chaos, create distrust in U.S. institutions, and target the preexisting divisions in the country. All this makes it harder for the United States to form a unified response to counter Russia in more traditional domains.

Misinformation and Disinformation Campaigns

Americans are regularly confronted with fake news in many forms from both domestic and foreign sources. There is a spectrum of false content online, from well-meaning friends on Facebook thoughtlessly sharing misinformation they assume to be true to more malevolent and targeted propaganda-like content designed to intentionally confuse and deceive. Therefore, it is important to understand the difference between the terms *disinformation* and *misinformation. Disinformation* is the malicious and intentional development and propagation of false information, while *misinformation* is the inadvertent spreading of erroneous content. Russia relies on both. A misinformation campaign, for example, could be employed maliciously by relying on unwitting users to spread false information.

Bill Gates, when asked in 1995 about false information spreading on the then-new "Net," stated that fake news would be easy to debunk because there would be more people checking the facts and information would be spread from friend to friend, a more trustworthy transaction.[21] But as we now know, it is this very aspect of social media that allows for misinformation campaigns to succeed and for fake news to flourish. Another core challenge

that makes online influence operations so successful is that once information is disseminated and consumed, it is hard to retract it from people's minds. The tools that make social media so useful for connecting, sharing, and organizing are the same tools that allow malign actors to take advantage and manipulate. This fact—paired with a need for fast news without waiting for validating research or fact-checking, the ease of sharing on social media platforms, and the fact that the most divisive topics are deeply emotional (for example, public health and race relations)—makes the United States the perfect target of this type of social media weapon.

Russia's modus operandi for social media exploitation is predictable: Identify a contentious issue, employ bots and trolls on various social media platforms to spread divisive rhetoric, amplify debates, and promote discord.[22] One of the most publicized influence operations by Russia was its interference in the U.S. elections in 2016. But Moscow's efforts are broader than elections and exist as part of an ongoing deliberate campaign against the U.S. public. As a diverse, pluralist society, the existence of societal fissures for target are numerous.

In 2019, leaked documents revealed that Russia considered targeting one of America's deepest and oldest fault lines as a nation: race. Documents showed Russia considered training African-Americans in combat and sabotage before returning these individuals to the United States to create a Pan-African state in the southern United States, physically breaking apart the country. The proposal, which was never enacted, intended to "destabilize the internal situation of the [United States]."[23] Russia recognizes that slavery and the resulting centuries-long inequality is the original American sin and the ultimate fissure to be exploited. Russian influence operations were used against African-Americans in advance of the 2016 election,[24] and more recently Russia has exploited the Black Lives Matter movement by flooding Twitter hashtags—a technique used to dilute legitimate related content, thus inhibiting the social media platform as a means of

communication during protests.[25] It is important to note that Russia's goal is rarely to promote one side of any issue, but to stir the pot and enflame tensions—U.S. self-destruction would be Russia's ideal victory.

Russia's information warfare tactics are a moving target, making them difficult to understand and counter. In June 2020, a large-scale, persistent 6-year-long disinformation campaign out of Russia was exposed. The campaign used new methods for targeting the West and Ukraine on issues ranging from denying Russian doping in international sporting events to the broader praising of Russia and its government and highlighting U.S. and NATO aggression and interference in other countries.[26] The campaign was labeled "Secondary Infektion"[27] as an homage to Operation Infektion, a Cold War callback to the 1980s disinformation campaign when the Soviet Union employed malicious messaging to sell the conspiracy theory that the U.S. military created the AIDS virus as a tool of war.[28] Of particular interest in Russia's methods during Secondary Infektion was the large number of "burner" accounts used for a single misleading tweet and then abandoned. As opposed to previous efforts to build social media accounts with a following, credibility, and trust, this shows Russia's recognition of Americans' media illiteracy, inability to recognize fake news, and unwillingness to research deeper than a single tweet. Few people take the time to seek the source of information, and so far Russia has been proved correct in its hypothesis.[29] As much as can be understood about Russia's goals and methods, the inexpensive and ubiquitous nature of social media empowers disinformation efforts to shift and flex to changes in the social media algorithms as needed. It could also release prolific amounts of false and harmful information, which, if only marginally successful, could have an outsized impact.

Amplifying Public Health Debates

Russia clearly recognizes how to identify, exploit, and amplify U.S. political tensions and the Nation's racial wounds

Transportation systems technicians from 452nd Logistic Readiness Squadron prepare 50 pallets of ventilators provided by U.S. Agency for International Development for delivery to Moscow, Russia, at March Air Reserve Base, California, May 19, 2020 (U.S. Air Force/Keith James)

as well as other seams and fissures. Public health is another area of acute debate in the United States, and one that is ideal for Russian targeting. Public health issues are both personal and societal, and therefore any discussion of related topics is often full of emotion and an eagerness to quickly obtain information. Often, people are more trusting of health advice from friends, family, or influencers they trust than impersonal institutions. A National Institutes of Health study found that "in the [United States], eight in ten Internet users search for health information online, and 74 percent of these people use social media."[30] This makes public health issues such as COVID-19 or measles an ideal target for Russian social media weaponization. It is divisive and emotional, and could realistically physically weaken the United States.

The anti-vaccination (anti-vaxxers) movement espouses a belief that vaccinations are at best unnecessary and at worst cause physical harm, including autism and seizures. The movement is fueled by a deep mistrust of authority and the existence of echo chambers online that encourage the spread of misinformation quickly and among friends. All the fake news about vaccines is actually harder to counter due to their amazing success. Diseases such as measles are seen as relics of the past that have long been eradicated and do not touch modern U.S. society. However, the United States is experiencing the greatest number of measles cases since 1992 in parts of the country where a significant percentage of the population has opted out of vaccines.[31] Vaccines are successful with herd immunity when, depending on how contagious the disease, a certain percentage of the society is vaccinated in order to protect a small number of the society who cannot get vaccines for various reasons (for example, children, pregnant women, and other vulnerable populations).

For a disease as contagious as measles, herd immunity occurs only if approximately 94 percent of a population is vaccinated; even a small change in vaccination numbers could bring back this disease, declared eliminated in the United States in 2000.[32] The result of erroneous fear-mongering about vaccines is a society that is physically degraded by previously eliminated diseases.[33] And now that the world grapples with the novel coronavirus causing COVID-19, large pockets of society are loathe to be told how to protect themselves and their communities. If Americans are rebelling against the science that underlies why masks and physical distancing are good preventative measures, it is foreseeable that there will be skepticism over a vaccine once it is available. The United States has been lulled into a false sense of security due to the very success of vaccines.

These public health crises would be atrocious enough without attempts by foreign adversaries to exacerbate them. The *Journal of Public Health* uncovered that the same Russian Internet Research Agency—led by Yevgeny Prigozhin (a close friend of Russian President Vladimir Putin) and indicted in Robert Mueller's investigation report on Russian election interference—was also behind deploying bots and trolls to spread disinformation on vaccinations.[34] In its analysis, the journal article notes that Russian bots and trolls tweeted an equal number of pro- and anti-vaccine tweets. The goal, it seems, was to stir the debate and bring people into their corners, further entrenching their own viewpoints. Russia's goal is to amplify and normalize the debate and firmly cement divisions. The health repercussions that result from a normalized vaccination debate were unlikely Russia's primary goal—merely a byproduct—but the fact that Russia could so callously degrade the health of U.S. citizens as a secondary effect of its influence operations is egregious. Given the ties to the Russian president, it presents further concerns about how this campaign may be endorsed by the state and what that means for how the United States responds. Deniability, however, is the crux of Putin's success in this area.

Russia has similarly used its predictable tactics against the United States to stoke fear and chaos and to undercut the U.S. response during the COVID-19 pandemic. False narratives spread by Russian state media, trolls, and bots range from conspiracy theories that the virus was variously created by migrants, as a U.S. bioweapon, or to benefit the U.S. pharmaceutical companies, or that the virus itself is a hoax.[35] Furthermore, China's disinformation use—which has historically been focused on domestic propaganda and creating the narrative that China and its authoritarian government are benevolent and powerful—has borrowed from Russia's influence operations playbook during the pandemic, moving from its initial propaganda-type response downplaying and denying the disease to all-out conspiracy theories and disinformation, including that the virus

was brought to Wuhan by the U.S. Army during Olympics-style military games in 2019.[36] This adds to concerns that Russia's influence operations are attractive to other U.S. adversaries and will continue to be a prime method of attack from multiple actors.

These attacks on public health present a threat to homeland and national security. The anti-vaxxer movement risks increasing U.S. vulnerability to infectious diseases. Looking forward to how these same tactics may be used against a COVID-19 vaccine once it is available, we must consider the implications of malignant messaging about vaccines from both domestic and foreign sources. Beyond propagating doubt in U.S. institutions (for example, hospitals/testing and government organizations such as the Centers for Disease Control and Prevention), these campaigns result in doubt of basic science (for example, people not wearing masks and possibly not trusting a future vaccine). By amplifying public health debates and not advocating for one side, Russia has helped normalize a previously fringe discussion rejecting basic science underlying vaccines and disease prevention. U.S. health institutions are faced with a crisis of trust as scientific facts about these contagious diseases are degraded by both intentional and inadvertent lies.

There are longer term effects of amplifying the anti-vaxxer movement. Beyond the health and institutional concerns, there are also costs to the U.S. health system, as well as costs associated with quarantining. The movement is a distraction for healthcare professionals who are overburdened in this crisis as it is, and for local, state, and Federal governments that must devote time and resources to countering this false information. Furthermore, natural or intentional biothreats (including natural biothreats exacerbated by foreign adversary messaging) could potentially inhibit the military's ability to project power abroad. The pandemic has shown how vulnerable forces are to contracting diseases such as COVID-19, and there is renewed awareness of this threat by our adversaries.[37] The United States has

also relied on the military to help with expanded hospital bed capacity at home, all of which stretches resources and in theory means fewer forces deployed.[38]

If anti-vaxxers grow in number and/or influence, this could weaken the U.S. ability to respond to any type of biological threat—natural or human-made. Bioweapons of the future are less likely to be those agents historically weaponized and will likely target civilian populations. Biological agents have always been difficult to weaponize because of the quantity and dissemination needed to have widespread, mass impact. As the large-scale programs of the Cold War gave way to the terrorist threat, the biothreat scenario of a biological agent–filled test tube dropped in a subway has been overtaken by disturbing real-world pandemic scenarios.

Russia and other U.S. adversaries are certainly noting U.S. vulnerabilities in its response to the coronavirus. All this presents renewed concerns of a future biological weapon, the effects of which could be further enabled by information warfare. These indiscriminate information attacks on public health reveal how Russia will exploit any divisions within the United States, even to the point of wreaking public health havoc. These attacks on public health highlight the type of ruthless adversary the United States faces. At a certain point, the United States must contemplate whether this interference in its public health is a biothreat caused by a foreign adversary.

Countering the Influence of Influence Operations

Asymmetric warfare is being waged against the United States and its citizens daily across multiple platforms and with expanded notions of what constitutes acceptable warfare. Though the effects of Russia's information operations on health matters are grave, we have not yet codified these societal attacks as warfare, and therefore they do not rise to the level of military response. The United States requires a comprehensive, whole-of-government solution to counter these actions as well as a whole-of-society awareness to be part

Berkut (Ukrainian riot police) man checkpoint at entrance to Crimean Peninsula, March 10, 2014 (Courtesy Sasha Maksymenko)

of the solution. Governments and companies could raise barriers to make the efforts harder, and people could be better informed on how to identify misinformation and disinformation, thereby making it less effective. The combined effects could lead to reducing Russia's influence, if not deterring it altogether. The solution will be complex, at all levels of society, and it begins and ends with an informed public with high media literacy.

Government can help but cannot alone solve the problem of disinformation any more than it can solely solve public health challenges. The 2020 National Defense Authorization Act called for the Director of National Intelligence to create a Malign Foreign Influence Response Center to coordinate and integrate across the Intelligence Community on issues of foreign influence; as of this writing, this center has not yet been established

as authorized.[39] In the past, there has been work to counter Russian messaging in pockets of the U.S. Government, but it has often been limited to addressing overt propaganda rather than the low-level guerrilla exploitation of social media we face today. During the Cold War, the U.S. Active Measures Working Group was established not only to counter Soviet disinformation but also to sensitize societies to be able to recognize Russian interference for themselves.[40] It would seem this type of whole-of-government commitment to countering disinformation would be timely to revive, perhaps in the form of the Malign Foreign Influence Response Center. Even so, it would not be enough on its own and certainly not with intelligence-only participation. The Department of State's Global Engagement Center is doing its part to identify, expose, and counter disinformation, but without higher visibility by U.S.

citizens and the Nation's adversaries, it cannot be fully successful.[41]

One of the most effective things that the U.S. Government could do to counter disinformation is practice consistent messaging and, in the case of disinformation and public health, deliver a consistent, science-based message. During the aftermath of the attempted assassination of Sergei Skripal in the United Kingdom using Novichok, Russia put out hundreds of conflicting narratives to confuse, deflect, and deny its involvement. The United Kingdom, rather than play whack-a-mole by attempting to disprove each falsehood, put out a consistent, science-based message that helped reveal the lies and inconsistencies within the Russian messaging.[42]

Furthermore, the United States must call out Russia for its cross-domain misdeeds, including in the area of information operations. The United States

must respond directly to these threats through targeted sanctions, international condemnation in multilateral forums, and other asymmetric responses. Despite Russia's attempts at deniability of its role in these campaigns, the United States and its allies should present evidence in a forum such as the United Nations Security Council to show the links between these bad actors and the Russian government. Because of Russia's veto on the Security Council, no resolutions would be passed, but this high-visibility action would highlight to the world Russia's malign activities and perhaps rally support of other nations around stopping this bad actor. The United States needs to assess Russia's actions not only by its methods but also by its effects. If Russia's social media meddling results in a physically weakened society, even inadvertently, the United States must consider treating these actions as more akin to a bioattack than to a cyber attack.

Industry partners would play an important role in the solution. Silicon Valley, the home of the platforms on which this misinformation and disinformation spreads, struggles with balancing the hazards of fake news with freedom of speech and shareholder pressure and therefore has not done nearly enough to combat the information warfare waged on social media sites. As a democratic society, we will not be able to shut down this threat but rather must accept that this false content exists and focus on empowering companies and users to identify and expose this content. In the midst of COVID-19, Twitter implemented a new system to identify and draw attention to articles and posts that may be considered dangerous or spreading disproven information. In June 2020, Twitter slapped a fact-check on Chinese Ministry of Foreign Affairs official Lijian Zhou's tweet advertising a bioweapon conspiracy theory. While this social media policing is fraught with censorship and free speech concerns and a "whack-a-troll" approach is inefficient, it is a good first step to draw users' attention to the reality that all tweets, even from verified accounts, must be read with a healthy dose of skepticism.[43]

As social media continues to evolve into more visual platforms including TikTok, it will be important to flag manipulated media such as artificial intelligence–enabled deepfakes. Though it presents a great challenge, as the technology to create believable deepfakes improves, so does the technology to counter it. Tech companies are investing in methods that reveal clues for when an image has been altered, such as water droplets on an image, a tell-tale sign of media manipulation.[44] There are also algorithms to assess when the title of an article does not match the content, which could then alert users and discourage them from sharing misleading information based on the title alone.[45] Incorporating these technologies into social media platforms to flag manipulated media before it is shared further would both slow the spread of false information and help create a society with a healthy level of skepticism and improved media literacy. To maintain freedom to access all information, we must ensure users have the tools they need to help recognize and counter disinformation.

The most important change that must happen to effectively counter Russian disinformation is an educated and empowered U.S. population capable of identifying and discrediting Russian disinformation. Deterrence will not work to stop or slow Russia's disinformation efforts; the United States should therefore focus on inoculating the population against Russia's attempts to influence the information domain. A challenge of countering disinformation during a public health crisis is balancing the need for a media-literate society that is highly attuned to detect false information, while inherently trusting institutions in equal measure. The United States must invest in media literacy and instill an awareness of the methods and goals of these targeted campaigns. In addition to making the public aware of Russia's role in these targeted information attacks, Americans must assess other fissures in U.S. society that might be targeted in this manner in the future.

Russia's theory of the United States is that its diversity is its weakness. To counter this narrative, the United States must show strength in its pluralism and work as a country to heal the divisions that make it the ideal target for this methodology. Russia is drilling deeper into the preexisting fault lines of American society—distracting, dividing, and weakening. Particularly in the face of the Presidential election and a modern pandemic, all Americans must be vigilant in questioning where information originates and hyperaware of the seams and fissures in American society that are primed for this type of attack. Healing the wounds and divisions of an increasingly polarized nation will go a long way toward protecting the United States from Russia's social media weaponization. **JFQ**

Notes

[1] Roy Godson, *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*, Hearing Before the Select Committee on Intelligence of the U.S. Senate, 115th Cong., 1st sess., 2017, available at <www.intelligence.senate.gov/sites/default/files/hearings/S%20Hrg%20115-40%20Pt%201.pdf>.

[2] Adam Taylor, "Did Russia Interfere in Brexit? An Unpublished Report Roils UK Politics Before Election," *Washington Post*, November 5, 2019, available at <www.washingtonpost.com/world/2019/11/05/did-russia-interfere-brexit-an-unpublished-report-roils-uk-politics-before-election/>; Filippa Lentzos, "The Russian Disinformation Attack That Poses a Biological Danger," *Bulletin of the Atomic Scientists*, November 19, 2018, available at <https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/>; Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vols. I and II (Washington, DC: Department of Justice, March 2019), available at <www.justice.gov/storage/report.pdf>.

[3] Tedros Adhanom Ghebreyesus, speech delivered to the Munich Security Conference, Munich, Germany, February 15, 2020, available at <www.who.int/dg/speeches/detail/munich-security-conference>.

[4] Godson, *Disinformation*.

[5] Svetlana Savranskaya and Tom Blanton, *NATO Expansion: What Gorbachev Heard* (Washington, DC: National Security Archive, 2017), available at <https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gor-

Marines fire 81mm mortar during training in support of Operation *Inherent Resolve* in Hajin, Syria, August 4, 2018 (U.S. Air Force/Corey Hook)

bachev-heard-western-leaders-early>.

⁶ *Ukraine: Background, Conflict with Russia, and U.S. Policy*, R45008 (Washington, DC: Congressional Research Service, April 29, 2020), available at <https://fas.org/sgp/crs/row/R45008.pdf>.

⁷ Gerard Toal, *Near Abroad: Putin, the West, and the Contest Over Ukraine and the Caucasus* (New York: Oxford University Press, 2017).

⁸ David M. Adamson and Julie DaVanzo, *Russia's Demographic 'Crisis': How Real Is It?* (Santa Monica, CA: RAND, 1997), available at <www.rand.org/pubs/issue_papers/IP162.html>; Cheney Kalinich, "Russia: The Sickness of a Nation," *The Yale Global Health Review* (Fall 2016), available at <https://yaleglobal-healthreview.com/2016/12/21/russia-the-sickness-of-a-nation/>.

⁹ Eugene Rumer, *Primakov (Not Gerasimov) Doctrine in Action* (Washington, DC: Carnegie Endowment for International Peace, 2019), available at <https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254>.

¹⁰ Bureau of Public Affairs, *Soviet "Active Measures": Forgery, Disinformation, Political Operations*, Special Report No. 88 (Washington, DC: Department of State, 1981), available at <https://www.cia.gov/library/readingroom/docs/CIA-RDP-84B00049R001303150031-0.pdf>.

¹¹ Dmitry Adamsky, "Strategic Stability and Cross-Domain Coercion: The Russian Approach to Information (Cyber) Warfare," in *The End of Strategic Stability? Nuclear Weapons and the Challenge of Regional Rivalries*, ed. Lawrence Rubin and Adam N. Stulberg (Washington, DC: Georgetown University Press, 2018).

¹² Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, 2013, available at <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>; Valery Gerasimov, "The Value of Science in Prediction," *Voenno-Promyshlenni Kuryer* 26, no. 840 (February 26, 2013), available at <www.vpk-news.ru/articles/14632>.

¹³ Valery Gerasimov, trans. Harold Orenstein and Timothy Thomas, "The Development of Military Strategy Under Contemporary Conditions: Tasks for Military Science," *Military Review* (October 2019), available at <www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2019-OLE/November/Orenstein-Gerasimov/fbclid/IwAR18VUoZTZ15KB7AvBVyPEAqCqo5w-5myuuymQPRqQ5qogem5JDR5PjsLCmA/>.

¹⁴ Carolina Vendil Pallin, "Internet Control Through Ownership: The Case of Russia," *Post Soviet Affairs* 33, no. 1 (2017).

¹⁵ Jane Wakefield, "Russia 'Successfully Tests' Its Unplugged Internet," BBC, December 24, 2019, available at <www.bbc.com/news/technology-50902496>.

¹⁶ Steven Erlanger, "Russia's RT Network: Is It More BBC or KGB," *New York Times*, March 8, 2017, available at <www.nytimes.com/2017/03/08/world/europe/russias-rt-network-is-it-more-bbc-or-kgb.html>; Nathan Layne, "U.S.-Based Russian News Outlet Registers as Foreign Agent," Reuters, February 7, 2018, available at <www.reuters.com/article/us-usa-trump-russia-propaganda/u-s-based-russian-news-outlet-registers-as-foreign-agent-idUSKCN1G201H>.

¹⁷ "Russia Tests Direct-Ascent Anti-Satellite Missile," *U.S. Space Command Public Affairs*, April 16, 2020; Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: CNA, September 2016), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf>.

¹⁸ David Lee, "The Tactics of a Russian Troll Farm," BBC, February 16, 2018, available at <www.bbc.com/news/technology-43093390>.

¹⁹ Elizabeth Townsend, *Understanding*

Narratives for National Security: Proceedings of a Workshop (Washington, DC: The National Academies Press, 2018), available at <www.nap.edu/read/25119/chapter/1>.

[20] Matthew Shaer, "What Emotion Goes Viral the Fastest?" *Smithsonian Magazine*, April 2014, available at <www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/>.

[21] Tom Huddleston, Jr., "In 1995, Bill Gates Made These Predictions About Streaming Movies and Fake News on the Internet," CNBC, May 31, 2019, available at <www.cnbc.com/2019/05/31/bill-gates-1995-predictions-about-streaming-movies-fake-news.html>; Bill Gates and Terry Pratchett, "GQ&A: Bill Gates Talks to Terry Pratchett About the Future, the Microsoft Revolution and How to Become a Billionaire," *GQ*, July 1995.

[22] *The War on Pineapple: Understanding Foreign Interference in 5 Steps* (Washington, DC: Department of Homeland Security, 2019), available at <www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf>.

[23] Richard Engel, Kate Benyon-Tinker, and Kennett Werner, "Russian Documents Reveal Desire to Sow Racial Discord—and Violence—in the U.S.," NBC, May 20, 2019, available at <www.nbcnews.com/news/world/russian-documents-reveal-desire-sow-racial-discord-violence-u-s-n1008051>.

[24] Scott Shane and Sheera Frenkel, "Russian 2016 Influence Operation Targeted African-Americans on Social Media," *New York Times*, December 17, 2018, available at <www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html>.

[25] Mark Scott, "Russia and China Target U.S. Protests on Social Media," *Politico*, June 1, 2020, available at <www.politico.eu/article/russia-china-us-protests-social-media-twitter/>.

[26] *Secondary Infektion at a Glance*, 2020, available at <https://secondaryinfektion.org/report/secondary-infektion-at-a-glance/>.

[27] Ben Nimmo et al., *Graphika: Secondary Infektion*, 2020, available at <https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf>.

[28] Thomas Boghardt, "Operation INFEKTION: Soviet Bloc Intelligence and its AIDS Disinformation Campaign," *Studies in Intelligence* 53, no. 4 (December 2009), available at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf>.

[29] Lance E. Mason, Dan Krutka, and Jeremy Stoddard, "Media Literacy, Democracy, and the Challenge of Fake News," *Journal of Media Literacy Education* 10, no. 2 (2018), available at <https://digitalcommons.uri.edu/jmle/vol10/iss2/1/>.

[30] C. Lee Ventola, "Social Media and Health Care Professionals: Benefits, Risks and Best Practices," *Pharmaceutical and Therapeutics Journal* 39, no. 7 (July 2014), available at <www.ncbi.nlm.nih.gov/pmc/articles/PMC4103576/>.

[31] Centers for Disease Control and Prevention (CDC), "Measles Cases and Outbreaks," available at <www.cdc.gov/measles/cases-outbreaks.html>.

[32] Sebastian Funk, *Critical Immunity Thresholds for Measles Elimination* (London: Centre for the Mathematical Modelling of Infectious Diseases, October 19, 2017), available at <www.who.int/immunization/sage/meetings/2017/october/2._target_immunity_levels_FUNK.pdf?ua=1>.

[33] CDC, "Measles History: Measles Elimination," 2018, available at <www.cdc.gov/measles/about/history.html>.

[34] David A. Broniatowski et al., "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," *American Journal of Public Health* (October 2018), available at <https://ajph.aphapublications.org/doi/10.2105/AJPH.2018.304567>.

[35] Judy Twigg, "Coronavirus in Russia: How Putin's Disinformation Efforts Could Backfire at Home," *Bulletin of the Atomic Scientists*, March 31, 2020, available at <https://thebulletin.org/2020/03/coronavirus-in-russia-how-putins-disinformation-efforts-could-backfire-at-home/>.

[36] Chris Buckley and Steven Lee Myers, "As New Coronavirus Spread, China's Old Habits Delayed Fight," *New York Times*, February 1, 2020, available at <www.nytimes.com/2020/02/01/world/asia/china-coronavirus.html>; Steven Lee Myers, "China Spins Tale that the U.S. Army Started the Coronavirus Epidemic," *New York Times*, March 13, 2020, available at <www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html>; Department of Defense, "7th International Military Sports Council: Military World Games," 2019, available at <www.defense.gov/Explore/Spotlight/CISM-Military-World-Games/>; Sarah Jacobs Gamberini and Amanda Moodie, "The Virus of Disinformation: Echoes of Past Bioweapons Accusations in Today's COVID-19 Conspiracy Theories," *War on the Rocks*, April 6, 2020, available at <https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/>.

[37] Daniel C. Payne et al., "SARS-CoV-2 Infections and Serological Responses from a Sample of U.S. Navy Service Members—USS *Theodore Roosevelt*, April 2020," *Morbidity and Mortality Weekly Report* (Washington, DC: CDC, June 12, 2020), available at <www.cdc.gov/mmwr/volumes/69/wr/mm6923e4.htm>.

[38] Geoff Ziezulewicz, "The USNS *Comfort* Is Now Taking Covid-19 Patients. Here's What to Expect," *New York Times*, April 8, 2020, available at <www.nytimes.com/2020/04/08/magazine/hospital-ship-comfort-new-york-coronavirus.html>; Gamberini and Moodie, "The Virus of Disinformation."

[39] National Defense Authorization Act for Fiscal Year 2020, 116th Cong., § 1790, January 3, 2019, available at <www.intelligence.senate.gov/legislation/damon-paul-nelson-and-matthew-young-pollard-intelligence-authorization-act-fiscal-1>; Amy Klobuchar et al., "Letter to Secretary Esper, Director Ratcliffe, Director Wray, General Nakasone, and Acting Secretary Wolf," U.S. Senate, 2020, available at <www.klobuchar.senate.gov/public/_cache/files/1/d/1d99087e-0a26-4242-a0cf-a5867d208a18/D1FD0C7DAF35260CBB-3D51CAB10A3324.062620disinformationletter.pdf>.

[40] Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Strategic Perspectives 11 (Washington, DC: NDU Press, 2012), available at <https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf>.

[41] Department of State, "Global Engagement Center," 2020, available at <www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/>.

[42] Tom McTague, "Britain's Secret War with Russia," *The Atlantic*, December 3, 2019, available at <www.theatlantic.com/international/archive/2019/12/britain-russia-nato-disinformation/602836/>.

[43] Nina Jankowicz, "Russian Trolls Are Only Part of the Problem," *New York Times*, January 25, 2018, available at <www.nytimes.com/2018/01/25/opinion/russian-trolls-fake-news.html>.

[44] Fijoy Vadakkumpadan and Ye Liu, *Detecting Deepfakes and Disinformation* (Cary, NC: SAS, 2020).

[45] Ibid.

Commodore Grace M. Hopper, USN (covered), popularized idea of machine-independent programming languages that led to development of COBOL, January 20, 1984 (U.S. Navy/James S. Davis)

Recruiting Cyber Specialists
Why the Services Must Modernize Qualification Standards

By Jesse P. Samluk, Mark A. Boeke, and Marcus A. Neal

Hardly a day goes by without another data breach concerning peoples' sensitive information—such as Social Security numbers, dates of birth, and payroll information—making the news. Billions of dollars are lost each year to data breaches and theft of intellectual property. Unfortunately, there is no end in sight. Despite our best cyber security efforts, criminal hackers seem to be one step ahead. Playing catchup to hackers is an infinite game of wits, brains, luck, and patience.

The uniformed services (to include here the Coast Guard, U.S. Public Health Service Commissioned Corps, and National Oceanic and Atmospheric Administration [NOAA] Commissioned Officer Corps) are also doing their version of playing catchup by forming their own siloed cyber elements.[1] Cyber issues are by definition not geographically bound, and they do not have a certain aspect to them that begs for assistance from any particular service component. This effort is *compounded* with the services recruiting and retaining cyber specialists in a decades-old personnel environment with even older medical, age, and prior service standards.

The uniformed services realize that cyber is its own distinct warfighting

---

Dr. Jesse P. Samluk is a Reserve Organization of America Member and an RF Engineer with the Department of Defense (DOD). Mark A. Boeke is a Lessons Learned Program Manager with DOD. Marcus A. Neal is a Lead Cyber Security Engineer with DOD.

domain, just like the land, sea, or air, where either nation-states or terrorist actors can target our country. It is a unique battlefield where no one receives direct fire, but the potential havoc created by a cyber attack could be more damaging than other forms of engagement. Cyber warfare does differ in that it knows no boundaries; even if the United States withdrew all its forces from foreign countries, it would still be vulnerable to cyber lines of operation from capable actors—both external and internal. Additionally, our assets in space are prime targets for hacking. Protecting the data of the recently established U.S. Space Force will place an additional demand on critically overburdened cyber professionals.[2]

Cyber security is among the fastest growing job markets, and such expansion is expected to continue rapidly over the next few years. Nearly every facet of society is under attack from state-sponsored hackers, including Russian attacks on classified government networks and North Korean ransomware attacks on average Americans. In this vein, the services are looking for the best and brightest and are actively recruiting to protect our government's critical systems. In return, the services offer the honor and privilege of wearing the uniform and assisting the Nation. However, the services are also competing for people against private industry, with familiar company names such as Google, Facebook, and Apple, as well as less familiar ones such as CrowdStrike and FireEye, to secure sensitive information of all stripes. Although private-sector employers can pay top dollar to attract new talent, government agencies (Federal, state, and local) cannot. That is not to say that cyber security experts are averse to government service; highly skilled cyber security professionals serve in the Nation's military and clandestine services and are perhaps the world's most potent offensive and defensive hackers. U.S. Code Titles 10 (Armed Forces), 18 (Crime and Criminal Procedure), and 50 (War and National Defense) work in concert to allow government cyber security professionals to operate under authorities that private industry cannot—a major point of appeal.[3] That said,

promotion policies, frequent moves, long deployments, and less-than-competitive pay present retention challenges for cyber security experts in uniform—even more so for those who must support families.

To address this problem, the uniformed services are starting to adapt in innovative ways. The Army already offers direct commissioning into the cyber field and is considering expanding direct commission ranks through colonel (O6), while also paying accession and retention bonuses between $40,000 and $100,000.[4] General Paul Nakasone, USA, while in his previous role as commander of U.S. Army Cyber Command, agreed that the current level of direct commission ranking (O2) is hampering recruiting and retention efforts. He stated, "We are limited to bringing [cyber specialists] in as a first lieutenant, and so we would like greater flexibility on that."[5] Considering that the Public Health Service Commissioned Corps already direct commissions the Surgeon General and Assistant Secretary for Health at the flag officer ranks of vice admiral (O9) and admiral (O10), respectively, this problem, while somewhat controversial for the Public Health Service Commissioned Corps, should be a nonissue for the rest of the services.[6]

Even marching band members in the Air Force, as an incentive to join the band, are rapidly promoted to E6 after initial training.[7] The Army is considering letting cyber personnel leave the military, learn new skills in private industry, and reenter service.[8] This concept is not unlike training with industry programs—an existing option for selected servicemembers. Lieutenant General Lori Reynolds, former commander of Marine Corps Forces Cyberspace Command, has stated, "We need to start thinking outside the box on some of this stuff, because, monetarily, it's really difficult to keep up with what industry offers."[9] While some of the ideas presented here are outside the box, the uniformed services have not changed their extremely restrictive medical, age, and prior service standards, even though the need is so great. Therefore, the purpose of this article is to argue and demonstrate that, given the urgent need for recruiting and retaining

cyber specialists, the time is at hand to make these necessary changes, so the uniformed services will be well prepared to defend our Nation in cyberspace. The clarion call is more revolutionary than evolutionary.

Medical Standard Barriers

In addition to meeting technical qualifications, cyber specialists also face other entrance standards that apply to all candidates: medical, age, and prior service reentry standards. No one is calling for the elimination of all criteria. The question is, what standards are appropriate for our modern and future cyber warriors?

The majority of current age-eligible prospects cannot meet the entrance standards; overall, this problem is catastrophic. According to a 2017 Pentagon report, 71 percent of those considered young enlistment age—that is, between the ages of 17 and 24—are ineligible to serve.[10] Of that number, close to 60 percent are ineligible due to either medical standards or physical fitness levels.[11] This problem is quickly becoming the next "looming national security crisis."[12] And of those deemed qualified to serve, only 15 percent exhibit any interest in service whatsoever.[13]

While the numbers are concerning, given the medical standards in their present state, it is also safe to say that most of the standards do not reflect the pace of advances in medicine. What was once considered a serious medical condition years ago can be treated successfully today. For example, consider a severe myopia condition from a detached retina as a result of an injury resulting from sports, a car accident, or even being a victim of an assault or other crime. Within the current medical standards, this particular eye condition is disqualifying and has a slim chance of receiving a medical waiver. Specifically, Department of Defense (DOD) Instruction 6130.03 disqualifies, "d. Retina. Any history of any abnormality of the retina, choroid, or vitreous."[14]

But eye surgery has improved over the years to treat such conditions so that a detached retina can be repaired, regardless of how it occurred. So, then, why are the uniformed services still regarding

some of these conditions as limiting for military service? Keep in mind that a detached retina is just one of many conditions that modern medicine has improved with consistent results, but the DOD instruction for medical standards has not evolved. That said, DOD has been known to evolve on the area of medical standards when there is a definite need: Due to a fighter pilot shortage, the Air Force no longer restricts applicants for being too short.[15]

The medical standards are written to treat everyone the same and to hold everyone to an equal standard regardless of military specialty. Not everyone can be or desires to be a fighter pilot, infantry, or even a special forces operator, which are specialties that require a stricter physical and specialized standard. Many who seek to join want to do something besides combat-related work. There are scores of other specialties in the services that people could join without being held to such stringent physical standards. In today's era, retired Army Major Scott Smiley continued to serve even after losing 100 percent of his vision after a suicide bomber attack in Iraq.[16]

The cyber domain is one of the specialties that does not require strict physical standards to do the job, and the uniformed services desperately need people to fill critical roles. Thus, the key question is whether the services will continue to perpetuate self-destructive and overreactive policies by maintaining questionably relevant standards. To further advance this point, conditions such as a detached retina (that has been corrected), previous back injuries (for example, herniated discs), asthma, or even eczema do not preclude a network operator from conducting a computer network attack on an adversary. Are the services willing to risk the exclusion of cyber experts because they have suffered injuries or have other minor medical conditions? Furthermore, do our adversaries reject technically gifted people because they have a medical condition that the uniformed services would consider a disqualifier?

A counterargument could be that the guidelines are strict to avoid any medical issues flaring up while the servicemember is deployed. That may be a valid case in some specialties, but servicemembers in cyber operations are generally in computing centers far away from any danger zone and could launch successful attacks with little more physical exertion than the touch of a keyboard and click of a mouse. Obviously, those cyber operators embedded in tactical units would need to meet more rigorous physical standards. Regardless, those members in cyberspace are dedicated to protecting systems and will go where they are needed. For this reason, *obsolete medical standards cannot be a barrier to recruiting cyber specialists if the uniformed services want to best achieve the offense—a principle of war.*

The solution is for the services to readily waive standards—as they often do for other critical specialties, such as physicians, lawyers, and chaplains—as long as these individuals can still perform the mission.[17] If waivers are required, then the process must be lean for shorter processing time. One possible way to speed up the process is to include retired military and civilian doctors' recommendations. Another proposed idea is to have an assisted accessions process in which applicants are evaluated holistically instead of just looking at a disqualifying condition on face value.[18] As an even better alternative, the services could adapt separate medical standards suited to the duties that would be performed as part of a particular specialty. Effectively, separate medical standards are already adopted today, in that troops in units such as the 75th Ranger Regiment meet higher standards than those of the Army in general. Case in point, rest assured that, regardless of medical issues, *these cyber professionals can still do the job.*

Age Standard Barriers

The same argument for outdated entrance standards could be made with age. Current guidelines for age vary by service but are mainly in place to ensure that 20 years of service can be completed when someone hits his or her sixties. To date, only the NOAA Commissioned Officer Corps has no age limit for applicants.[19] The Public Health Service Commissioned Corps allows nonprior military service applicants the highest maximum age cutoff: age 44.[20]

The uniformed services have shown an ability to adapt to adjusting outdated age standards when faced with filling a critical specialty. In 2018, Tyrone Krause, a 63-year-old cardiothoracic surgeon, was commissioned into the Navy at the rank of commander (O5).[21] If this surgeon can commission later in life, at a higher rank, then are age standards really necessary in an era where people live longer and are more vigorous well into their seventies and beyond?

For another example, consider Grace Hopper, who was born in 1906, earned a PhD in mathematics from Yale in 1934, and joined the Navy Reserve in 1943. She became a pioneer with the new compiled computer language COBOL in the 1950s.[22] Commander Hopper retired from the Navy Reserve in 1966 but was recalled to Active duty to continue her work with COBOL. Her second retirement was as a Rear Admiral, lower half, in 1986, when she was nearing age 80.[23]

The key point here is a familiar adage: "With age comes wisdom and experience." Even Commander Krause, at the time of his commissioning, stated, "A lot of people in the private sector have a lot of skills they can bring to the Navy and military in general. You can be 40 years old, 50 years old, and your profession may be something that's necessary. . . . You can certainly give back."[24]

Commander Krause's statement resounds within the cyber community. Would the services scoff at someone who has 25 years in the cyber arena just because he or she did not meet an age standard? Did the Navy deride former White House Chief of Staff Reince Priebus for an age waiver at age 46 to become a human resource officer in the Naval Reserve?[25] If the age limit has to do with ensuring 20 years of service just to earn a full pension, then that argument is now a moot point. The uniformed services implemented an agile forward-looking pension plan, known as the Blended Retirement System, which allows members to have their Thrift Savings Plan retirement account if they leave before 20 years of service.[26]

Captain Scott M. Smiley, first blind officer and second Wounded Warrior to hold position of command, passes guidon back to 1ˢᵗ Sergeant Deon E. Dabrio during U.S. Army Warrior Transition Unit at West Point change of command ceremony, February 1, 2010 (U.S. Army/Tommy Gilligan)

Trying to change age standards is nothing new. In 2012, Representative Paul Broun, Jr. (R-GA), tried to enact legislation that would allow people at any age to join the uniformed services as long as the candidates could meet minimum health and fitness requirements. The House at that time voted down the measure. Congressman Broun, a retired Navy medical officer, even stated that the age cap is "an arbitrary policy."[27] This age cap is also extended to Federal law enforcement agencies. These agencies, such as the Federal Bureau of Investigation, control key components of America's coordinated cyber efforts. Such agencies are also hampered by these restrictions, as a candidate must be younger than age 37, thus also eliminating that avenue for patriots of a certain age who still want to contribute.[28]

Counter to the proposed legislation eliminating an age limit is the argument made by Representative Susan Davis (D-CA) that "risks outnumber gains" and that older personnel are more likely to become injured and take longer to heal.[29] We must reject this age bias. The services seem perfectly happy and content to relax standards for medical personnel, as previously mentioned, so why not cyber? It is understood that medical professionals are always in demand, as they possess unique skills. So are cyber professionals. For instance, as medical devices become increasingly "connected," who is going to ensure that those devices are secure, especially in remote environments where lives are on the line? Is age really going to affect those sitting at a workstation performing information security?

There is some hope: Private industry is starting to see the value of older workers.[30] Even physically demanding and dangerous occupations akin to military service, such as career fire departments in major cities like Philadelphia, do not have age limits for new recruits.[31] For recruiting older cyber professionals, the Army wants to remove the retirement-age requirement, which could, in turn, render irrelevant the age restriction.[32] Additionally, in 2018 a relatively unnoticed request for comments in the *Federal Register* indicated that the services may be modifying the selective service process for those with "cyber skills, and science, technology, engineering, and mathematics skills for which the Nation has a critical need, without regard *to age* or sex."[33] While it appears that there may be a shift in thinking about age, the solution here is that the uniformed services need to reflect NOAA Commissioned Officer Corps policy on having no age limit in place. There is no reason to have an arbitrary age limit in place, especially with what we are up against in cyberspace.

Prior Service Barriers

Prior service barriers are also lasting administrative obstacles. There are

"The President's Own" U.S. Marine Band performs during retirement ceremony for General Thomas D. Waldhauser at Marine Barracks Washington, DC, September 27, 2019 (DOD/James K. McCann)

potential recruits with prior service who were discharged honorably, but something may have affected their reentry—perhaps a particular narrative statement or a reentry code on their discharge certificate. Some may even have been discharged under less-than-honorable conditions (such as a general discharge). Whatever the circumstances at the first discharge, those contexts may now be a moot point. It is not unheard of for some of these prior servicemembers to have turned their lives around and matured from when they were younger; today, they could be looking for a second chance to serve.

Unfortunately, the services would rather grant waivers to those who have more serious background problems, like felonies and drug use, than to take back those members who may have had minor issues similar to those aforementioned at the time of discharge.[34] Some of those

members seeking a second chance often serve in other ways, perhaps in the police force, as emergency medical technicians, or in career/volunteer fire departments; some have even deployed to dangerous areas alongside the uniformed services, albeit in a civilian role. These individuals have demonstrated themselves through selfless service in their communities and have put their lives on the line. There are even prior service cyber professionals who feel the calling to serve in the military yet again; however, it seems as though the services turn a blind eye to these individuals who want to return—and who have a clean record—because their narratives and/or reentry codes appear to be worse than felonious crimes or drug use. To say that the uniformed services place objective guilt on former members for matters that happened years ago and have since been corrected is an understatement. Because society in general—and the services in

particular—gives second chances to those who have committed serious crimes, *there is no reason for not giving a second chance to former members, discharged under adverse conditions, who have proved themselves.*

To address the current need, as the saying goes, "Desperate times call for desperate measures." And, indeed, we are in desperate times, especially on the cyber front. Although some may vigorously argue that the concern is solely a retention issue and not a recruitment issue—even though retention is in the forefront too—there is resounding evidence to the contrary that has even been acknowledged by Pentagon officials.[35] Even if the problem were solely a retention issue, recruiting is an inherent part of the process, and adjustments need to be made for the future.[36] Moreover, because there is a problem no matter what, DOD and other services are simply too selective when it comes to former uniformed

Sergeant Brittany Deturo, 401st Army Field Support Brigade, positions herself to practice deadlift element of new Army Combat Fitness Test during familiarization training at Camp Arifjan, Kuwait, August 17, 2020 (U.S. Army/Kevin Fleming)

servicemembers trying to help in this field. The solution is clear: Let those who have prior experience have a second chance. The need is too great in the cyber domain to be so fastidious.

Conclusion: Modernizing Standards

The future is ours to create the opportunity for talented, skilled, and driven people. In light of the current cyber situation, agencies of the U.S. Government are taking the challenge head-on, each and every day. In particular, the uniformed services have made serious headway to counter cyber adversaries. But significant obstacles remain, and the most important issue is attracting, recruiting, training, and retaining a world-class force of people to serve in this field in uniform. We need them if we are to gain and maintain the initiative—an offensive principle of war.[37]

To their credit, the services recognize that there is a big problem in this area. Some of the concern is based on compensation, but what the services fail to realize is that there are some cyber professionals out there who are not interested only in money. These professionals would sacrifice a higher salary in private industry, endure the prolonged application and boarding process, and get the necessary clearances and polygraphs just to have the honor of wearing the cloth of this Nation. These are the type of people that the uniformed services need—those who are loyal and will never give up. If the services could only seek out and recognize these individuals and give them a chance—or a second chance, in some instances—they could prove themselves and, without a doubt, make a real contribution to closing U.S. cyber deficiencies. Unfortunately, common sense does not necessarily prevail, and we are increasing

risk in this area just to maintain antiquated standards in the face of adversaries who seem to have the upper hand in the cyber domain. Our adversaries would gladly accept into their ranks a cyber operator who can wreak havoc but who also has a condition that the services would find disqualifying. Relating back to the principles of war, more and better talent allows us to gain and maintain the initiative in this battlespace, which we arguably have ceded.

Changing standards for the uniformed services is not unheard of; they have had a long history of adjusting or even ignoring standards to allow for talented recruits in specialized fields, and, given the nature of cyber warfare, it may even be possible to accept individuals with physical disabilities.[38] The services used to grant field commissions in times of need as well. Another possibility is that the services could also retrain those who

Civilian QF-4E Pilot/Controller Lieutenant Colonel Jim "Wam" Harkins, USAF (Ret.), hugs his wife, Annette, after being showered with champagne upon exiting cockpit of his McDonnell Douglas F-4 Phantom II for last time following ceremonial final military flight of storied aircraft at Holloman AFB, New Mexico, December 21, 2016 (U.S. Air Force/J.M. Eddins, Jr.)

are wounded and have limited means to serve in a fuller capacity. Instead of medically discharging these wounded warriors, the services should allow them to serve with honor and retrain them to engage in the cyber threats we face.

Some critics may argue that adapting standards for cyber personnel could affect overall readiness and that there are always civilian positions instead.[39] This argument stems from a larger problem surrounding the culture of the services—specifically the cultural biases of what a warrior looks like.[40] The counterargument is that future warriors will need science, technology, engineering, and mathematics skills in order to adapt to high-tech threats in real time.[41] There is a need for uniformed members under Title 10 authority whose jobs cannot be outsourced to contractors or civilians.[42] Furthermore, not everyone who joins the uniformed services, explicitly the Armed Forces, need be a "trigger puller." The Marine Corps' "President's Own" marching band musicians do not "attend recruit training or basic combat training because of their unique mission to provide music for the President and the Commandant [of the Marine Corps]."[43] These highly skilled musicians

also occupy permanent positions and hence cannot be transferred.[44] Perhaps our cyber model reflects the "President's Own" to a degree, but significantly more than the current model of the Marine Corps Cyber Auxiliary.[45]

To this end, it does take talented people to address the cyber problem. The services should consider themselves fortunate that people want to join them in the cyberspace community and should embrace these professionals with open arms, adjusting the standards to allow their entry. It would be a grave mistake to turn them away if the goal of the services is to "own" the boundless cyberspace. It will be difficult to defend against our adversaries in the cyber domain if the military continues to have unfilled cyber positions because of outdated standards. **JFQ**

The authors acknowledge the following individuals for their assistance in shaping this article: Lieutenant Colonel Susan Lukas, USAF (Ret.); Major Crispin Burke, USA; Lieutenant Colonel Chris Lusk, USA (Ret.); Cryptologic (Maintenance Branch) Chief Petty Officer Tim Paul, USN (Ret.); and Dr. Irene M. Zoppi Rodriguez.

Notes

[1] U.S. Cyber Command components include U.S. Army Cyber Command (headquarters in Fort Gordon, Georgia), Marine Corps Forces Cyberspace Command (headquarters in Fort Meade, Maryland), U.S. Fleet Cyber Command (headquarters in Fort Meade, Maryland), and Air Forces Cyber (headquarters in Joint Base San Antonio, Texas).

[2] Space Policy Directive–4, *Establishment of the United States Space Force* (Washington, DC: The White House, 2019).

[3] *U.S. Code,* available at <https://www.govinfo.gov/app/collection/uscode/2017/>.

[4] Kathleen Curthoys, "How the Army Is Competing with Google for These Ninjas," *Army Times*, August 6, 2018; Jeffrey E. Phillips, "'Lateral Entry': Direct Commissioning of Civilians, a Pro and Con," *ROA*, August 3, 2016, available at <https://www.roa.org/blogpost/1434064/253796/Lateral-entry—Direct-commissioning-of-civilians-a-pro-and-con>; Crispin J. Burke, "The Pentagon Should Adjust Standards for Cyber Soldiers—as It Has Always Done," *War on the Rocks*, January 24, 2018, available at <https://warontherocks.com/2018/01/pentagon-adjust-standards-cyber-soldiers-always-done>; Armed Forces Communications and Electronics Association (AFCEA), "U.S. Army Introduces Cyber Fast Track for Civilians," *AFCEA*, February 13, 2017, available at <https://www.afcea.org/content/Blog-us-army-introduces-cyber-fast-track-civilians>.

[5] Lauren C. Williams, "Military Looks for Ways to Bring in Cyber Talent at Better Salaries," *Federal Computer Week*, March 14, 2018.

[6] U.S. Department of Health and Human Services, "Leadership," available at <https://www.hhs.gov/about/leadership/index.html>; Richard Carmona, "Instant Admirals and the Plague of Politics in the United States Public Health Service: Back to the Future," *Military Medicine* 182, no. 5–6 (May 2017), 1582–1583, available at <https://doi.org/10.7205/MILMED-D-17-00039>.

[7] Air Force Bands, "Auditions and USAF Band Career Information," available at <https://www.music.af.mil/Bands/The-United-States-Air-Force-Band/About-Us/Careers-in-The-United-States-Air-Force-Band/Frequently-Asked-Questions/>.

[8] Kathleen Curthoys, "Army Cyber Should 'Let Nerds Be Nerds,' Experts Say," *Army Times*, October 11, 2017.

[9] Sean Gallagher, "DOD Needs Cyberwarriors So Badly It May Let Skilled Recruits Skip Boot Camp," *Ars Technica*, May 9, 2017, available at <https://arstechnica.com/information-technology/2017/05/dod-needs-cyber-warriors-so-bad-it-may-let-skilled-recruits-skip-boot-camp/>.

[10] Thomas Spoehr and Bridget Handy, *The Looming National Security Crisis: Young*

Americans Unable to Serve in the Military (Washington, DC: The Heritage Foundation, February 13, 2018), available at <https://www.heritage.org/defense/report/the-looming-national-security-crisis-young-americans-unable-serve-the-military>.

[11] *Ready, Willing, and Unable to Serve* (Washington, DC: Mission: Readiness, 2009), available at <http://cdn.missionreadiness.org/MR-Ready-Willing-Unable.pdf>.

[12] Spoehr and Handy, *The Looming National Security Crisis.*

[13] Dennis Laich, Jonathan Askonas, and Gil Barndollar, "The Armed Forces Arithmetic Isn't Adding Up," *The Hill*, December 6, 2018, available at <https://thehill.com/opinion/national-security/419641-the-armed-forces-arithmetic-isnt-adding-up>.

[14] Department of Defense (DOD) Instruction 6130.03, *Medical Standards for Appointment, Enlistment, or Induction into the Military Services* (Washington, DC: DOD, May 6, 2018), 12.

[15] Oriana Pawlyk, "The Air Force Will No Longer Reject Pilot Applicants for Being Too Short," *Military.com*, May 22, 2020, available at <https://www.military.com/daily-news/2020/05/22/air-force-will-no-longer-reject-pilot-applicants-being-too-short.html>.

[16] *Hope Unseen*, available at <https://hopeunseen.com/about/>.

[17] Burke, "The Pentagon Should Adjust Standards for Cyber Soldiers."

[18] Joe Schuman, "Department of Disqualified: Fixing the Broken Military Medical Accessions Process," *War on the Rocks*, November 20, 2018, available at <https://warontherocks.com/2018/11/department-of-disqualified-fixing-the-broken-military-medical-accessions-process/>.

[19] National Oceanic and Atmospheric Administration Commissioned Corps, "Frequently Asked Questions," available at <https://www.omao.noaa.gov/learn/noaa-corps/join/frequently-asked-questions>.

[20] U.S. Public Health Service Commissioned Corps, "How to Apply," available at <https://www.usphs.gov/how-to-apply>.

[21] J.D. Simkins, "Ensign Commissions Her 63-Year-Old Father as a Navy Officer," *Navy Times*, July 14, 2018.

[22] COBOL (common business-oriented language) was designed in 1959 by the Conference/Committee on Data Systems Languages and was partly based on the programming language FLOW-MATIC (the first English-like data processing language), which was designed by Grace Hopper.

[23] Yale University Office of the President, "Biography of Grace Murray Hopper," available at <https://president.yale.edu/biography-grace-murray-hopper>.

[24] Simkins, "Ensign Commissions Her 63-Year-Old Father as a Navy Officer."

[25] Mark D. Faram and Leo Shane III, "A 46-Year-Old Ensign Who Once Ran the White House?" *Navy Times*, December 14, 2018.

[26] "Uniformed Services Blended Retirement System," *Military Compensation*, available at <https://militarypay.defense.gov/blendedretirement/>.

[27] Jeff Ousley, "Military Age Restrictions: How Old Is Too Old to Serve?" *Veterans United*, June 21, 2018, available at <www.veteransunited.com/network/military-age-restrictions-how-old-is-too-old-to-serve/>.

[28] Federal Bureau of Investigation, "Frequently Asked Questions," available at <https://www.fbi.gov/about/faqs/how-old-do-you-have-to-be-to-become-an-agent?>.

[29] Ousley, "Military Age Restrictions."

[30] Erika Prafder, "Mature People Are Working Longer, and That's a Benefit for Companies," *New York Post*, June 24, 2018.

[31] Monica Peters, "The Philadelphia Fire Department Is Hiring," *The Philadelphia Sunday*, September 1, 2016.

[32] Carten Cordell, "Army Officials Are on the Hunt for More Cyber Talent," *Fed Scoop*, October 11, 2018, available at <https://www.fedscoop.com/army-cyber-officials-hunt-for-talent/>.

[33] Williams, "Military Looks for Ways to Bring in Cyber Talent at Better Salaries"; National Commission on Military, National, and Public Service, "Request for Information on Improving the Military Selective Service Process and Increasing Participation in Military, National, and Public Service," *Federal Register*, February 16, 2018, available at <https://www.federalregister.gov/documents/2018/02/16/2018-03261/request-for-information-on-improving-the-military-selective-service-process-and-increasing>. Emphasis added.

[34] Spoehr and Handy, *The Looming National Security Crisis*; Lolita C. Baldor, "Army Using Drug Waivers, Bonuses to Fill Ranks," *Army Times*, August 1, 2018, available at <www.armytimes.com/news/your-army/2018/08/01/army-using-drug-waivers-bonuses-to-fill-ranks/>.

[35] Justin Lynch, "Why Recruiting Cyberwarriors in the Military Is Harder Than Retaining Forces," *Fifth Domain*, November 1, 2018, available at <www.fifthdomain.com/dod/2018/11/01/why-recruiting-cyber-warriors-in-the-military-is-harder-than-retaining-forces/>.

[36] Isaac R. Porche et al., *Cyber Power Potential of the Army's Reserve Component*, RR-14900-A (Santa Monica, CA: RAND, 2017), available at <https://doi.org/10.7249/RR1490>.

[37] William T. Eliason, "An Interview with Paul M. Nakasone," *Joint Force Quarterly* 92 (1st Quarter 2019), 4–9.

[38] Burke, "The Pentagon Should Adjust Standards for Cyber Soldiers."

[39] Mark Cancian, "Blue-Haired Soldiers? Just Say No," *War on the Rocks*, January 18, 2018, available at <https://warontherocks.com/2018/01/blue-haired-soldiers-just-say-no/>.

[40] Jacquelyn Schneider, "Blue Hair in the Gray Zone," *War on the Rocks*, January 10, 2018, available at <https://warontherocks.com/2018/01/blue-hair-gray-zone/>.

[41] Ibid.

[42] Raj M. Shah, *Military Service Hearing: Creating New Pipelines to Service and Fostering Critical Skills*, Testimony Before the National Commission on Military, National, and Public Service, Washington, DC, May 16, 2019, available at <https://inspire2serve.gov/_api/files/268>.

[43] Patrick Cirenza, "The President's Own as a Model for the Marine Corps Cyber Auxiliary," *War on the Rocks*, September 18, 2019, available at <https://warontherocks.com/2019/09/the-presidents-own-as-a-model-for-the-marine-corps-cyber-auxiliary/>.

[44] Ibid.

[45] U.S. Marine Corps, "Marine Corps Established Volunteer Cyber Auxiliary to Increase Cyberspace Readiness," *Marines*, May 13, 2019, available at <https://www.marines.mil/News/Press-Releases/Press-Release-Display/Article/1845538/marine-corps-establishes-volunteer-cyber-auxiliary-to-increase-cyberspace-readi/>.

Atlas V rocket launches Navy's Mobile User Objective System 2 satellite from Space Launch Complex—41 at Cape Canaveral Air Force Station, Florida, July 19, 2013 (U.S. Navy/NASA/Patrick H. Corkery)

Space Operations
Lines, Zones, Options, and Dilemmas

By Jerry V. Drew

Major Jerry V. Drew II, USA, is a Planner in the U.S. Army Space and Missile Defense Command.

While there is considerable literature available on both the strategic and tactical aspects of space operations, there is surprisingly little that discusses the linkage of tactical space operations to the achievement of strategic objectives through operational art. In addition to government documents such as the National Security Space Strategy, influential academic works have largely focused on the strategic and political aspects of the space domain.[1] Much of the professional literature produced by military practitioners, on the other hand, has focused on the tactical exploitation of space systems.[2] While this collection of works sometimes hints at the possibility of synchronizing tactical action to achieve strategic ends, none provides a practical explanation of how commanders and staffs might achieve such a feat.

Furthermore, the doctrinal publications that bear some responsibility for this explanation—for instance, Joint Publication 3-14, *Space Operations* (2018), and U.S. Army Field Manual 3-14, *Army Space Operations* (2019)—tend to develop domain-unique language rather than language rooted in theoretical principles that is translatable across other warfighting domains.[3] As a result, the connective tissue of a common operational language between space operations and the rest of the joint force is largely missing. With the recent establishment of U.S. Space Command and the U.S. Space Force, the joint force stands poised to

expand its incorporation of the space domain into existing and future operations. To effectively accomplish this expansion, however, operational art as it applies to the space domain requires a deeper conceptual consideration—one that leverages and expands on existing warfighting concepts to enable multidomain integration.

The literature of operational art itself has a long history and provides much of the language necessary for such a consideration. In 1838, the Swiss general and theoretician Baron Antoine-Henri Jomini published *The Art of War*, a work that permeated the U.S. military of the 19th century and forms the basis for the modern doctrinal lexicon. Like his contemporary, the Prussian general Carl von Clausewitz, Jomini concerned himself primarily with land warfare, but his concepts remain relevant to applications of space systems in modern warfare. Indeed, they have served the theoreticians of warfare quite well over the past two centuries. Within the realm of military space literature, Everett Dolman's *Astropolitik* makes reference to the sea power theory of Alfred Thayer Mahan, himself a disciple of Jominian thought.[4] Furthermore, John Klein's *Space Warfare* leverages the writings of Sir Julian Corbett, whose *Some Principles of Maritime Strategy* was a reaction to Mahanian thought.[5] When taken as a whole, the existing body of theory provides rich source material from which to discuss the ways one might employ military space systems within the larger context of operational art. The operational artist may then apply these concepts to work toward an understanding of how space systems, along with systems centered in other domains, contribute to an overall strategic goal. From the perspective of space systems, the most important among these concepts are lines of communication (LOCs), lines of operation (LOOs), zones of operation (ZOOs), and zones of communication (ZOCs). While these concepts have theoretical, historical, and doctrinal precedent in the land, maritime, and air domains, they take on a new form in the context of the employment of space systems.

Lines of Communication

In *The Art of War*, Jomini simply defines *LOCs* as "the practicable routes between the different portions of the army occupying different positions throughout the zone of operations."[6] Clausewitz provided more detail. In *On War*, he writes that LOCs "lead from an army's main position back to the main sources of food and replacements."[7] They allow for the conduct of various functions, including resupply, troop movement, delivery of mail, transit of couriers, and the conduct of administrative action. The joint doctrinal definition of LOCs follows the vein of the Clausewitzian theory but falls short on two accounts. First, it acknowledges only the troop movement and resupply functions of an LOC. Second, it concedes the domain-specific or multidomain nature of LOCs insofar as they apply to the land, maritime, and air domains, but offers no consideration of the concept as it applies in the space (to say nothing of the cyber) domain.[8]

In an effort to expand these concepts into the space domain, Klein defines *celestial lines of communication* (CLOCs) "in and through space used for the movement of trade, materiel, supplies, personnel, spacecraft, electromagnetic transmissions, and some military effects."[9] Thus, Klein's CLOCs maintain similar functions to those of Clausewitz and include "physical CLOCs" that launch satellites or replenish constellations and the "nonphysical LOCs" of radio communications links.[10] While traditional LOCs can perform all the Clausewitzian functions, Klein's nonphysical CLOCs are a special type of nondoctrinal line in that they perform only the information transmission function. These communications links fulfill the courier functions mentioned by Clausewitz, but unlike the LOCs of 19th-century wars, nonphysical CLOCs are not tethered to supply routes.

In his effort to map warfighting concepts to the space domain through the creation of new terminology, Klein provides the joint force a great service. The downside of his approach, however, is that the language he creates is domain specific, rather than domain inclusive.

Additionally, because of the specificity required to describe them, the terms themselves are somewhat cumbersome. If one considers the function of the lines rather than their physical location, however, one may arrive at terms that more easily translate to other components of the joint force. These functions, which Clausewitz defined and which Klein addresses, are the transfer of personnel and materiel (in the manner of the joint doctrinal definition of the concept) and data transfer. Klein's concept of physical CLOCs provides justification for the inclusion of space domain LOCs into the joint doctrinal definition of LOCs; like LOCs in other domains, the physical CLOCs perform the function of transferring personnel and materiel from one location to another. For this reason, one may simply consider Klein's physical celestial LOCs as LOCs per the doctrinal definition, retaining the modifier "celestial" when useful. Also, Klein's nonphysical CLOCs transfer data. As such, the term *data line of communication* (DLOC) seems more useful because it describes the function of the concept while remaining general enough to apply to other domains, including cyber. Thus, "nonphysical celestial lines of communication" simplify to "data lines of communication."

The concept of LOCs when applied to the space domain—both in its relation to theoretical notions and in its uniqueness from current doctrinal definitions—carries tremendous significance for the operational artist. First, space-specific LOCs are a concern to the military planner if constellation replenishment is a concern. Historically, constellations receive new satellites as older models fail—a very deliberate process that requires significant lead time. In a protracted conflict that witnesses the destruction or degradation of vital space systems, however, a belligerent may endeavor to launch replacement capabilities. Massive satellites require large rockets to lift them into orbit, which in turn necessitates significant infrastructure. In the case of the United States, large rocket launches occur either over the eastern coast of Florida or the western coast of California.

Crewman from 101st Airborne Division (Air Assault) stands beside AH-64A Apache helicopter armed with M-230A1 30mm automatic cannon and AGM-114 Hellfire missiles as it prepares for takeoff during Operation *Desert Shield*, January 23, 1991 (DOD)

In terms of LOCs, these launch sites represent a base, and the typical rocket flight and orbital path form the remainder of the LOC. As the trend toward smaller, more capable satellites continues, future constellation replenishment may not be dependent on traditional launch facilities but may employ ad hoc launch sites or launch-capable air and sea platforms. If ever realized, such launch options would give the operational artist greater flexibility in opening LOCs.

As for DLOCs, those provide tremendous flexibility to the operational artist. In a space domain context, such DLOCs allow for the control and use of the spacecraft. In support of multi-domain operations, the DLOCs allow for communication not only with a military force's rear area (in the Clausewitzian sense of LOCs) but also with other units operating in the same zone (in the more Jominian sense of LOCs). In contemporary U.S. military operations, the force largely takes for granted the ability to talk to rearward and adjacent units via satellite, but an enemy with jammers or antisatellite missiles could threaten such access. DLOCs, then, provide a concept for the operational artist to use in the deliberate planning and employment of space systems and of communications systems in other domains.

Lines of Operation

In theory and doctrine, the LOC and the LOO are related concepts that center on the friendly military force. Generally, LOCs lead from the massed force rearward and connect terrain already traversed with rearward bases. LOOs, on the other hand, lay out the path that the force intends to follow to reach its objectives. In the words of Jomini, LOOs connect "the decisive points of the theater of operations."[11] As in Jomini, the doctrinal definition of *LOO* hinges on decisive points. In joint doctrine, a LOO connects actions "on nodes and/or decisive points related in time and [physical] space to an objective."[12] Whereas Jomini designates only physical locations as decisive points, the joint definition expands to include not only places but also events, critical factors, or functions.[13]

Whether adapting the concept of LOO from theory or doctrine, the employment of space systems through operational art requires consideration of LOOs and LOCs in and across multiple domains. Most obviously, space operations can occur *in* space. Just as

often—and sometimes simultaneously—space operations occur *to* or *from* space. DLOCs provide the electromagnetic connection between the ground station controlling the in-space action, between the satellite and the air or sea force executing along its LOO, or between the electronic warfare system and its satellite target. The penultimate operational artist would be capable of synchronizing the activity of LOCs and LOOs of all domains through integrated planning. For much of the joint force, however, space operations are not a familiar topic and require further explanation.

As in the other domains, an objective in space may be terrain based (attainment of a specific orbit or orbital slot) or enemy based (in the case of an antisatellite system that seeks to destroy another satellite). One terrain-based LOO might follow the mission's critical events: launch, attain orbit, transfer orbit, reach final orbit, begin proximity operations. With current technology, this LOO might take weeks or months to complete and significantly deplete the spacecraft's onboard fuel reserve. Any effort to synchronize the tactical actions of such a satellite, then, requires an understanding of these time-distance calculations and how those relate to operations in other domains. In the near future, one might imagine multiple satellites (or groups of satellites) executing independent LOOs. These formations may converge at their decisive point in space just as the air and land forces mass at their decisive points on Earth.

While the orbital aspect of space operations remains the most obvious, ground-based space operations forces may also execute along LOOs. The LOO of a satellite communications unit, for example, may begin with an intertheater deployment. Establishing an initial operating location follows. As the conflict escalates, the unit relocates to a more suitable position—either rearward, forward, or perhaps to an entirely different continent in order to maintain the DLOCs that are essential for the joint force to operate. Nondeployable space operations units (the so-called deployed-in-place units) may execute similar relocations, but because these

units are less mobile, their potential set of LOOs contains fewer options; they may plan only to move from point to point and then possibly back again. Regardless of their relative complexity, operations would likely require execution of multiple LOOs to maintain the viability of multiple DLOCs. It is therefore useful to define a concept that groups multiple LOOs and LOCs into sets.

Zones of Operation and Zones of Communication

Since LOOs are possible both in space and in the employment of space systems from Earth, ZOOs are also possible in both locales. A ZOO consists of multiple LOOs, and like a LOO, a ZOO could exist in any single domain or across multiple domains. Indeed, a ZOO may be multidomain in nature, including the orbital and surface-based space operations LOOs along with land, maritime, or air LOOs. The previous example of multiple satellites converging simultaneously with air and ground forces provides such a case. A *ZOO* is not a defined doctrinal term but a Jominian concept, "a fraction of the whole theater of war which may be traversed by an army in the attainment of its objective."[14]

Just as multiple LOOs may coalesce to form a ZOO, multiple LOCs may coalesce to form a ZOC, and multiple DLOCs may coalesce to form a data zone of communication (DZOC). Within the context of contemporary space operations, it is difficult to define a ZOC because the personnel and materiel transport functions are isolated—that is, major launch facilities are widely separated and not employed as complementary assets in a warfighting sense. With the expansion of responsive launch capability, however, such ZOCs may be possible. Additionally, in the near future, orbital refueling or repair satellites may traverse groups of well-defined LOCs in a manner similar to how fuelers and maintenance vehicles traverse well-worn road networks on the ground. For the present, however, the DLOC is the operative principle of space operations, and the DZOC therefore requires a more expansive consideration.

Figure 1. DLOC Between Single Satellite and Single Ground Station
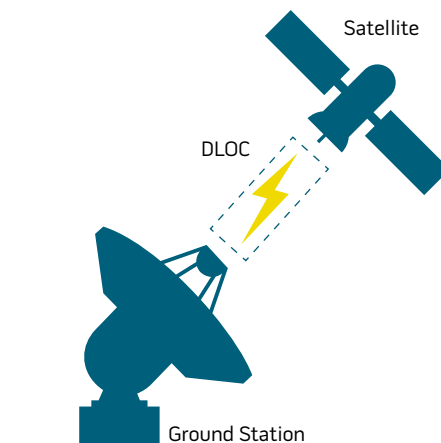
In the context of space systems, the simplest DLOC consists of the uplink or downlink signal between the ground and the satellite—in doctrinal terms, the link segment of the space system (figure 1). In modern military systems, however, the reality can be much more complicated.

A typical beam from a transmitting satellite (for example, a communications satellite) covers a large area on the ground. One need to think only of how many backyard satellite dishes a single communications satellite may service. Similarly, in military operations, one satellite may service many ground receivers within a single theater or even within multiple theaters. One may imagine radio waves linking the satellite transponder to each of the ground-based receivers within the footprint of the transmitted beam. This group of links forms a DZOC. Figure 2 shows a DZOC consisting of one satellite communicating with multiple receivers.

While one satellite may transmit to multiple receivers with a single transmitter, it is also possible for a satellite to have multiple transponders, each capable of servicing multiple receivers. In this situation, each transponder creates multiple links by transmitting to multiple receivers, each of which may be considered as separate DZOCs.

The visualization of DZOCs changes slightly depending on the orbital altitude of the satellite in question. For satellites in

Figure 2. DZOC of One Satellite and Multiple Receivers
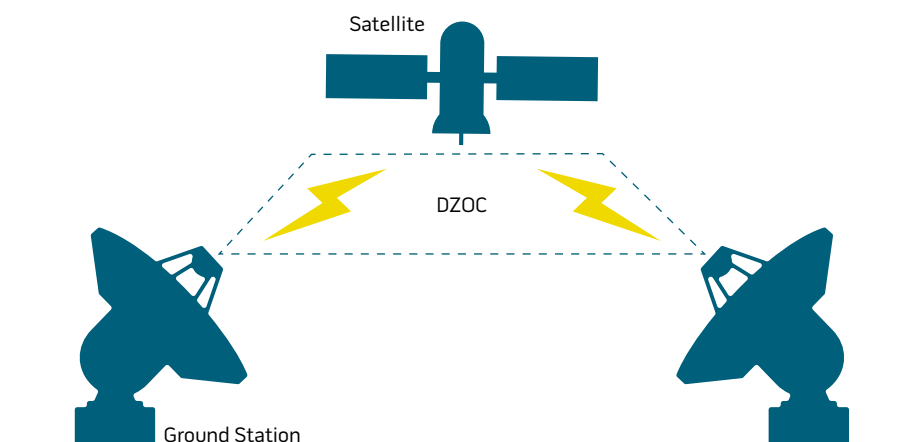
Figure 3. DZOC Changes as Satellites Move
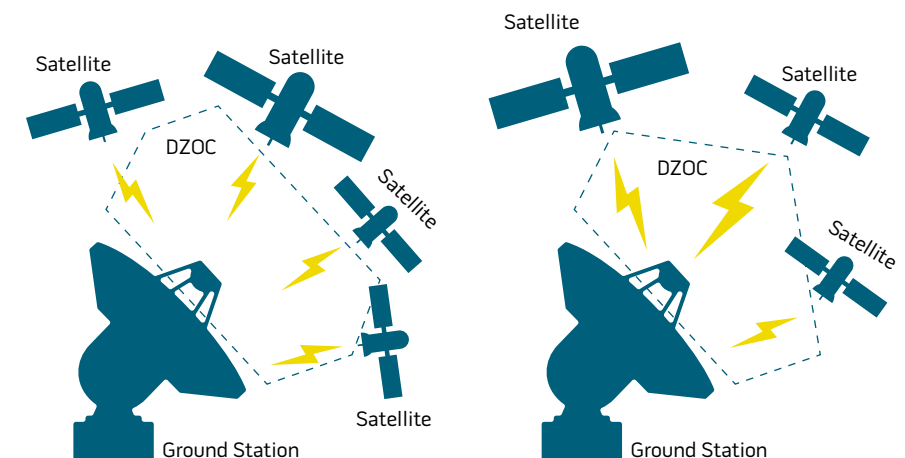
geosynchronous earth orbit (GEO), the satellite remains in view of the same locations on Earth. Its orbital speed matches the rotational speed of Earth, giving an observer on the ground the perception that the satellite is stationary over that point. For satellites at this orbital altitude, the ZOC is continuously operational. As altitudes become lower, the speed of the satellite relative to the ground increases. For low-Earth orbit (LEO) satellites, a few hundred miles from the Earth, a ground receiver will be able to access the satellite only for a short period, perhaps only several minutes. In this situation, the DZOC is short lived; it comes into existence when the links are established and is not reestablished until the next satellite in the constellation comes along or until the original satellite returns.

Between GEO and LEO resides a wide expanse of space called medium-Earth orbit (MEO). The GPS constellation resides in MEO (approximately 12,000 miles from the Earth) and is designed to provide multiple links to handheld and vehicle-mounted receivers. As one might deduce from the in-between altitude, the windows during which to access GPS satellites are neither constant (as with GEO satellites) nor very brief (as with LEO satellites). Although access times vary depending on the location of the receiver relative to the constellation's configuration, a single GPS satellite typically remains in view for 3 to 6 hours. For an accurate solution, each receiver requires access to four satellites, but more than the minimum are typically in view. As one satellite dips

below the horizon and out of view of the receiver, another will likely have risen above the horizon to offer its own link, thus providing a continuous solution to the receiver.

Unlike the typical receivers depicted in the first two DZOC illustrations, GPS receivers accept simultaneous input from multiple satellites. Thus, the DZOC involves multiple transmitters, not multiple receivers. Figure 3 shows the changing DZOCs as GPS satellites move relative to the ground observer.

As with missile warning, weather, intelligence, and communications satellites, GPS satellites enable tactical operations and have historically operated with little enemy interference. As long as these enabling means are working normally and the space domain remains relatively uncontested, the operational artist may be tempted to devote less consideration to the vulnerabilities of such space systems. However, when a system becomes degraded, the synchronization of operations with windows of system capabilities becomes a significant concern.

Options and Dilemmas

The line of communication and the line of operation serve as foundational concepts for joint force operations. In this sense, space operations are not different from operations in the other domains, but the application of familiar concepts to a different domain requires clarifying and expanding their application. With the building blocks of LOCs, DLOCs, LOOs, ZOCs, DZOCs, and ZOOs in place, one must consider how to employ them in a larger operational context. While one may apply these concepts within any number of operational frameworks, a historical example of large-scale combat—the Persian Gulf War—provides an illustration of how such concepts can apply, particularly in creating options for the friendly force and dilemmas for the enemy.

Jomini states as the first point of his fundamental principle that the aim of war is to mass combat power at the decisive point.[15] To do this effectively, even with a joint force operating in multiple domains, the complementary concepts of options

Navy's fourth Mobile User Objective System satellite, encapsulated in 5m payload fairing, stands mated to Atlas V booster inside Vertical Integration Facility at Cape Canaveral's Space Launch Complex–41, August 19, 2015 (Courtesy United Launch Alliance)

and dilemmas apply. One may imagine Napoleon arriving at the preordained time of battle with three corps converging on the enemy army. With three corps at his disposal, Napoleon had options. For example, he could have attacked with two while keeping the third in reserve. Alternatively, he could have used two for a turning movement while employing the third as a guard force. He also could have used two as an enveloping force while sending the third against a weaker enemy detachment.

An enemy commander with five corps could have parried every dilemma presented by Napoleon with forces to spare. In other words, he or she would have retained options in the face of multiple dilemmas. Retaining options in the face of dilemmas is the essence of flexibility.[16] All other things equal, an enemy with only two corps would have had fewer options: conduct a deliberate defense, withdraw, or split the force to risk a bold

offensive—as Robert E. Lee did successfully at the Second Battle of Bull Run in 1862.[17] If employed with simultaneity, however, Napoleon's three corps could theoretically present more dilemmas than the enemy's two corps could absorb. When one force presents an enemy force with multiple, synchronized dilemmas along the depth of the enemy force, the enemy's entire ability to wage war effectively becomes overwhelmed; the friendly force has achieved operational shock.[18]

One way for the joint force to create dilemmas is to open multiple ZOOs that the enemy must address. As previously mentioned, these zones may or may not correspond to domains. In the case of the Gulf War, for example, U.S. Central Command opened land and air ZOOs from Saudi Arabia and a maritime ZOO in the Persian Gulf.[19] Arguably, the air assault of the 101st Airborne Division on the allied coalition's northern flank represented a cross-domain zone of

operation.[20] The ability of allied coalition forces to open multiple ZOOs and effectively sequence operations within those ZOOs imposed on the Iraqi armed forces a state of operational shock. In essence, the allied coalition presented the Iraqis more dilemmas than they could effectively counter, and the advantages of space-based intelligence, communications, missile warning, and navigation directly contributed to the ability of the allied coalition to maintain an overwhelming operational tempo.

As far as the space domain is concerned, little unclassified information is available on how the United States did or did not open space zones during the Gulf War.[21] It is important to consider, however, that multiple LOOs had placed all the space systems into operation over a period of decades preceding the conflict, and it is possible that the U.S. Air Force adjusted satellites during the conflict to maximize their usefulness. While LOOs

Sodium Guidestar at Air Force Research Laboratory Directed Energy Directorate's Starfire Optical Range provides real-time, high-fidelity tracking and imaging of satellites too faint for conventional adaptive optical imaging systems, November 17, 2005 (DOD)

and ZOOs may not have been the operative concept for the planned use of space systems during the Gulf War, space systems did provide DLOCs for weather, intelligence, and missile warning, and DZOCs for communications and a not fully operational GPS constellation.[22]

Imagine now a similar scenario in which a near-peer belligerent is able to counter U.S. forces in the land, sea, and air domains and perhaps overmatch U.S. forces in the cyber domain. In such a scenario, how does the operational artist employ space systems? As in the Gulf War, the operational artist must consider possible and existing lines and zones and make provisions for opening and maintaining them through the deliberate placement of assets within the specific strategic context. While the employment of existing assets may be more or less straightforward, employing new satellites presents a difficult problem.

While it may be possible to accelerate or reprioritize launch and on-orbit testing timelines, military satellites typically require long lead times for operational employment. For this reason, the planning and employment of such constellations falls more within the realm

of strategy, but the destruction of such assets poses immediate problems for both the operational artist and the tactician.[23] While the tactician must adjust procedures to the capability of the remaining resources, the operational artist must understand the strategy and work to readjust the means to enable the most effective strategy. Operational planners (particularly military space professionals), then, must understand the vulnerabilities of space systems and develop contingency plans to address their loss. Furthermore, with the limitations of satellite replenishment in mind, one may plan to counter the enemy's satellite replenishment capability by cross-domain attacks on launch facilities or by cyber action against the enemy's industrial base.

Unlike the operational employment of enabling means (satellites for communications, intelligence, among others), the operational employment of offensive orbital systems requires a different calculus. First, orbital antisatellite systems, inspector satellites, or manipulator satellites are niche capabilities that have existed since the Cold War—albeit in low numbers and largely in an experimental rather than operational capacity.[24] Still, a

consideration of their potential is useful. Based on the desired target, the distance they are required to travel, and their design specifications, there is a tradeoff between how far an orbital asset could travel and how fast it could get there. As with the infantry Soldier, a satellite may travel a long distance slowly without expending all its fuel, or it may travel a short distance very rapidly with a greater expenditure. Satellite refueling, however, is not currently practicable, and any future LOO that involves offensive orbital means must bear the limitations in mind. Nonetheless, in theory, a belligerent may use multiple spacecraft-based robotic manipulators to open multiple LOOs, thus forming a zone of operation and presenting the enemy with an additional dilemma set.[25] A less complicated—and perhaps a more operationally useful—way of establishing a ZOO is from Earth through the employment of defensive space control (DSC) or offensive space control assets.

If an in-space ZOO is one type of space operation ZOO, a second type is a defensive space control ZOO. Given the fundamental importance of information transmission to the joint force, the

employment of DSC assets should be an early consideration for the operational artist. As mentioned, DSC assets may be placed outside or inside the theater of war to protect the most necessary data lines or zones. The effort to deploy, emplace, and operate these assets constitutes a contributing LOO, the ultimate goal of which is to establish a DLOC with the intent of monitoring an already existing link segment. The employment of multiple assets into multiple theaters represents additional LOOs and additional DLOCs that may, if mutually supporting, coalesce into data zones (figure 4).[26]

A third type of ZOO, a combination of offensive space control LOOs, involves the employment of satellite jammers. As with DSC assets, a force may develop multiple LOOs (or ZOOs) with the ultimate goal of establishing offensive LOCs in the theater of war, from an external theater or in multiple and mutually supporting theaters. The combination of multiple offensive DLOCs constitutes an offensive DZOC, and depending on the orbital motion of the target satellites, the operational artist must determine the appropriate sequencing of the tactical offensive actions to contribute to the overall strategic effect. Alternatively, if an enemy force is establishing offensive DLOCs, the operational artist must anticipate which friendly assets are vulnerable and take action to mitigate operational risk.

Conclusion

An understanding of space operations across the joint force is now more essential than ever, and achieving this understanding depends on a language that translates concepts across all domains. Necessarily, this effort must not focus on the creation of domain-unique language (as has the space doctrine of the past) but on making similar concepts relatable so that domain-specific practitioners across the joint force can communicate effectively with one another. The language of operational art—with some expansion of existing concepts like lines of operation and communication—provides the connective tissue to link the operations of all domains through theoretical ideas that enable practical application.

Figure 4. Multiple DLOCs Coalesce to Form DZOC
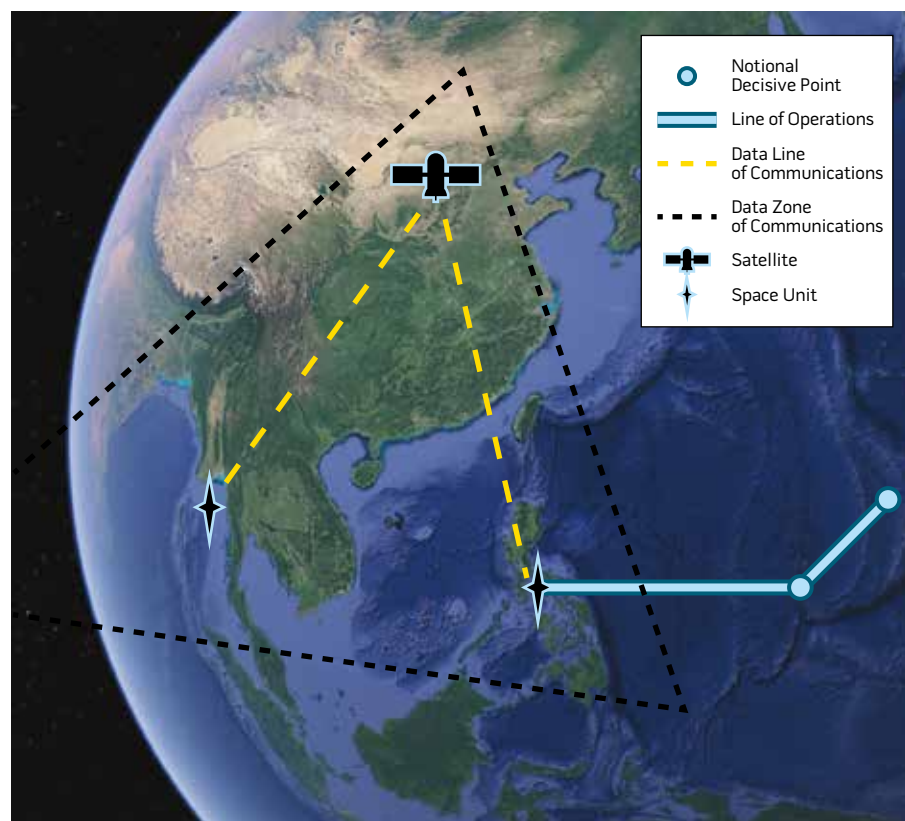
To begin addressing the practical questions of how operational artists may employ space systems, theory and doctrine provide a starting point from which to consider specific new concepts. Historical examples provide context and, in the case of ZOCs, suggests a useful concept neither in traditional theory nor in U.S. doctrine. That the ideas of Jomini come to the fore indicates his importance in creating the language of modern military operations as evidenced in the theoretical writings of Mahan, Corbett, and Klein. However, while each of these writers focused on a particular domain, in contemporary warfare, domains are inseparable, and domain-specific theories of warfare may be misleading. Theory, history, and doctrine all posit that it behooves a belligerent to present as many dilemmas as possible to an enemy across all domains (simultaneity) while maintaining as many options as possible for one's own force (flexibility). While it is possible that the forces of a single domain may be able to achieve the desired ends,

it is unlikely—and perhaps even foolish—for any modern nation to operate in that way. Indeed, all domains are essential in modern warfighting, and the operational artist must approach the goal of victory through the establishment of ZOOs in as many domains as possible, the maximal use of ZOCs, and the synchronization of activity across all domains. ZOCs and ZOOs provide the friendly force options while forcing the enemy to confront multiple dilemmas, and the creative process of integrating multidomain ZOCs and ZOOs is fundamental to operational art. Indeed, the creative process that links the tactical actions to the strategic ends is ongoing and requires continuously revisiting one's understanding of operations in all domains.[27] For this reason, concepts—whether they come from history, theory, or doctrine—may be more important tools for an operational artist in the conduct of warfighting than any domain-specific means. **JFQ**

Notes

[1] See, for example, Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (Abingdon, UK: Frank Cass Publishers, 2002); Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007); James Clay Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*, 2nd ed. (Stanford: Stanford University Press, 2011).

[2] Of note, the Air University's *Space Primer*, a decade's worth of *Army Space Journal*s published during the height of the Iraq War years, and multiple master's theses and monographs from both the Naval Postgraduate School and the Command and General Staff College endeavored to expound on the tactical usefulness of space.

[3] Joint Publication 3-14, *Space Operations* (Washington, DC: The Joint Staff, April 10, 2018); U.S. Army Field Manual 3-14, *Army Space Operations* (Washington, DC: Headquarters Department of the Army, October 2019)

[4] Dolman, *Astropolitik*, 33.

[5] John J. Klein, *Space Warfare: Strategy, Principles, and Policy* (New York: Routledge, 2006), 3.

[6] J.D. Hittle, ed., *Jomini's Art of War* (Harrisburg, PA: Stackpole Books, 1965), 78–79.

[7] Carl von Clausewitz, *On War*, eds. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 345.

[8] According to joint doctrine, a line of communication is "a route, either land, water, and/or air, that connects an operating military force with a base of operations and along which supplies and military forces move." See Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, as amended through February 15, 2016), 141.

[9] Klein, *Space Warfare*, 51.

[10] Ibid., 52–53. A celestial line of communication (CLOC) should be voiced as "clock" to avoid confusion with a sea line of communication (SLOC).

[11] Hittle, *Jomini's Art of War*, 78.

[12] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 141.

[13] Ibid., 60.

[14] Hittle, *Jomini's Art of War*, 78.

[15] Ibid., 67.

[16] In Army doctrine, the tenets of unified land operations are flexibility, depth, synchronization, and simultaneity. Neither joint nor Army doctrine formally defines these terms. See Field Manual 3-0, *Operations* (Washington, DC: Headquarters Department of the Army, 2017), 5-5.

[17] Allan R. Millett, Peter Maslowski, and William B. Feis, *For the Common Defense: A Military History of the United States from 1607 to 2012* (New York: Free Press, 2012), 174.

[18] Shimon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (Abingdon, UK: Frank Cass Publishers, 1997), 18.

[19] Robert H. Scales, *Certain Victory: The U.S. Army in the Gulf War* (Fort Leavenworth: U.S. Army Command and General Staff College, 1994), 84, 390–391, figure 5-3. I also must acknowledge Dr. Bruce Stanley, associate professor at the School of Advanced Military Studies, for first explaining to me the concept of lines, zones, and dilemmas, which he did in the context of the Gulf War. The additional consideration of lines and zones in the space domain is my expansion of the concept.

[20] Ibid., 221.

[21] Except for three pages of overview on the general conclusions of the study, the portion of the *Gulf War Air Power Survey* regarding space operations remains classified. Eliot A. Cohen et al., *Gulf War Air Power Survey*, vol. 4 (Washington, DC: Government Printing Office, 1993), v–vii.

[22] James Walker, Lewis Bernstein, and Sharon Lang, *Seize the High Ground*: *The Army in Space and Missile Defense* (Washington, DC: U.S. Army Space and Missile Defense Command, 2003), 151–157.

[23] Dolman, *Astropolitik*, 61. Much of Dolman's discussion in *Astropolitik* engages this aspect of "astrostrategy."

[24] See, for example, Jim Sciutto and Jennifer Rizzo, "War in Space: Kamikazes, Kidnapper Satellites and Lasers," CNN, November 29, 2016, available at <www.cnn.com/2016/11/29/politics/space-war-lasers-satellites-russia-china/>; Andrew Ogilvie et al., "Autonomous Satellite Servicing Using the Orbital Express Demonstration Manipulator System," fact sheet, Defense Advanced Research Projects Agency, 2008, 25–29.

[25] A celestial zone of operation (CZOO) is voiced as "kazoo" not as "sea zoo."

[26] Although the tendency in the joint force is to view the deployment of forces *to* a combat theater as administrative—indeed, Service component commands perform this function through their administrative control authorities—planners should treat such moves as operational so as not to downplay the need for synchronization with the overarching scheme of maneuver or to negate the possibility of enemy interference. As the Marines state, a force must be able to "fight to the fight."

[27] Huba Wass de Czege, "Thinking and Acting Like an Early Explorer: Operational Art is Not a Level of War," *Small Wars Journal*, March 14, 2011; Naveh, *In Pursuit of Military Excellence*, 13.

Members of USS *Normandy* visit, board, search, and seizure team brief Navy Secretary Kenneth Braithwaite on seizure of illicit shipment of advanced weapons and weapon components intended for Houthis in Yemen, February 9, 2020 (U.S. Navy/Alexander C. Kubitza)

The Strategic Potential of Collected Exploitable Material

By Michael R. Fenzel with Leslie Slootmaker and R. Kim Cragin

In November of 2007, I was commanding an infantry battalion in the Eastern Paktika Province of Afghanistan. One of our convoys was hit by an improvised explosive device (IED) on a routine mission in the border district of Bermel, just a few short miles from Pakistan. A brilliant young troop commander (Captain David Boris, USA, age 30) and his dependable and tough driver (Sergeant Adrian Hike, USA, age 26) were killed in the explosion.[1]

A few questions came to mind as I struggled with the loss. Who had built and placed the IED? How could I exact justice? What actions could I take to prevent a recurrence? This is the timeless dilemma of every commander in combat. It is personal. It does not matter that the attack occurred in a time of war. It is of no consolation to understand "the enemy has a vote." Thirteen years later, as I reflect back, it was this searing event and my talented staff's response that taught me the value of collected exploitable material (CEM).[2]

After the Bermel attack, an explosive ordnance disposal (EOD) team conducted a postblast analysis of the site and found what would prove to be critical

Major General Michael R. Fenzel, USA, is Vice Director for Strategy, Plans, and Policy (J5). Commander Leslie Slootmaker, USN, is assigned to the Directorate for Strategy, Plans, and Policy (J5), Global Integration, at the Pentagon. Dr. R. Kim Cragin is a Senior Research Fellow at the Center for Strategic Research, Institute for National Strategic Studies, at National Defense University.

Afghan National Army soldiers, combined with assets from 45th Infantry Brigade, conduct cordon and search in village thought to be home to IED makers and Taliban fighters, August 21, 2011, in Alingar District, Laghman Province (DOD/Ryan Crane)

CEM. Specifically, the EOD team collected a pressure plate with metal soup can lids and wire taped together at one end. The team also recovered fragments of a battery pack wrapped in goat hair. Biometrics (fingerprints) were lifted from the tape. In addition to the EOD team, I had a retired Federal Bureau of Investigation (FBI) agent serving on my staff. He informed me that the same fingerprints had been discovered at the site of four other IED attacks. He explained how the distinctive configuration of these IEDs was the "signature" of a single bombmaker. If we could locate him, then we would have the person responsible for killing Captain Boris and Sergeant Hike.

Five months later, a local goat herder told us that bombs were being made in a *qalat* (a fortified place) in Bermel. A combined Afghan army and coalition team searched the dwelling and found the same distinctive bombmaking materials. The bombmaker and his fellow insurgents were detained, taken to prison

in Kabul, and, based on evidence derived from the CEM, convicted of terrorism charges under Afghan law. We subsequently saw an immediate and dramatic reduction of IED activity in Bermel.

This story is not uncommon. The Armed Forces often acquire large quantities of CEM in the midst of operations. Even now, we hold over 300 terabytes of CEM gathered from across the globe.[3] It has become common practice for ground force commanders to use CEM as they "find, fix, finish" violent extremist organizations (VEOs) on the battlefield.[4] Less frequently, and outside of conflict zones, law enforcement authorities have used CEM in criminal proceedings against a wide variety of illicit actors. CEM has proved useful in securing longer prison sentences for convicted terrorists and persuading countries to extradite terrorists to the United States. Yet CEM has its challenges. Transfers or "warm handoffs" between the U.S. military, law enforcement, and other government agencies

have been inefficient and cumbersome.[5] The Armed Forces also have struggled to get these materials to our allies and partners in a usable format and timely manner.[6]

To address these challenges, Secretary of Defense Mark Esper in January released new guidance on CEM in a memorandum titled "Classification of Materials Captured, Collected, or Handled by the Department of Defense." The memo directs that all new CEM be unclassified unless sensitive sources, methods, or activities were used to acquire it.[7] The document articulated the following logic:

Sharing of CEM with foreign partners is often necessary to effectively prosecute persons who pose a clear and present danger to the safety and security of the United States and our foreign partners in civilian courts of law. . . . Unclassified CEM is releasable to the public and partner nations to support the U.S. mission objectives

and partner nation security and law enforcement purposes, to include criminal prosecutions.[8]

This new guidance lays the foundation for CEM to be used well beyond the battlefield. It allows for easier transfer of CEM from the military to other U.S. Government agencies, as well as our allies and partner nations. Yet substantially more work needs to be done. This article argues that, to realize its full potential, CEM also should be leveraged as part of strategic competition.[9]

To do this, the article first examines recent efforts by the Armed Forces to acquire CEM during operations against VEOs and transfer it to law enforcement authorities in the United States, our allies, and partner nations. The article explores three different types of CEM: al Qaeda's internal memos and correspondence gathered in conjunction with the Abbottabad raid, IED components collected as part of "Omar's Cache" in Baghdad, and, more recently, so-called Islamic State (IS) registration forms captured during Operation *Inherent Resolve*. Second, the article discusses how the lessons learned from these counter-VEO operations apply to strategic competition. In doing so, the article provides some concrete, albeit limited, examples of how the Armed Forces have used CEM to counter Iran's malign activities and how a similar approach could be taken with Russia and China. The article concludes with an appeal to the joint force to think more creatively about the application of CEM, in combination with other instruments of National power, to confront rogue states and revisionist powers.

Lessons Learned from the VEO Fight

In May 2011, Army aviators and Navy SEALs executed a raid against then–al Qaeda leader Osama bin Laden's compound in Abbottabad, Pakistan. The SEALs killed bin Laden and captured over 470,000 electronic files from his compound.[10] These documents represent the most well-known recovery of CEM by the Armed Forces in modern history.

But that is not the end of the story. One of the Abbottabad documents linked Saleh al-Somali, al Qaeda's then–head of external operations, to an individual named Abid Naseer. Naseer was already in a British prison at the time of the raid.[11] He was arrested in April 2009, along with three other terrorists for plotting attacks on behalf of al Qaeda in New York City, Manchester, and Copenhagen.[12] British authorities extradited Naseer to the United States, and U.S. prosecutors were able to use documents from the Abbottabad raid to secure a 40-year prison sentence for him.[13] This example illustrates how CEM can assist prosecutors in their efforts to connect individual terrorists to foreign VEOs and their global terrorist networks. It also underscores the critical need for the Armed Forces to appropriately classify (certainly not misclassify) these types of materials at the point of collection in order to preserve the ability of prosecutors to use CEM in civilian criminal courts.

This same logic—that is, making CEM available for criminal proceedings—recently enabled the extradition of a bombmaker from Turkey to the United States, as well as his successful prosecution in Arizona. Syrian terrorist Ahmad Ibrahim Al-Ahmad built IEDs for Iraqi insurgent groups to use against the Armed Forces deployed to Iraq during Operation *Iraqi Freedom*. Some of his devices were discovered during an August 2006 raid on an IED factory on 50 Omar Street in Baghdad.[14] We gathered these devices, colloquially referred to as "Omar's Cache," and, in partnership with the FBI, collected biometrics in anticipation of using this CEM in the future. This effort eventually proved its value. Unbeknownst to the United States, Al-Ahmad left Iraq in July 2010 and relocated to China. He continued to build and ship IED components to Iraqi insurgents while living there. But in May 2011, Al-Ahmad attempted to return to Iraq by way of Istanbul, and Turkish authorities arrested him. Three years later (2014), the U.S. Government persuaded Turkey to extradite Al-Ahmad to the United States for prosecution

based on the CEM found in Omar's Cache and an International Criminal Police Organization (INTERPOL) Red Notice.[15] By the time Al-Ahmad was extradited, he had shifted his allegiance from the 1920 Revolution Brigade to the Islamic State.[16]

Beyond prosecutions, the Armed Forces have provided CEM to allies and partner nations to assist with efforts to identify and arrest terrorist plotters before they can execute attacks in the West. As an example, in October 2015, the Armed Forces captured a cache of documents from IS and shared them with Danish authorities.[17] The cache contained registration forms from foreign terrorist fighters who had left their homes in Western Europe and traveled to the Middle East to join IS.[18] As it happens, IS is a highly bureaucratic VEO that uses payrolls, guest house registries, weapons inventories, leave requests, and registration forms. On the captured forms, IS required applicants to provide recruiters with their name, nationality, residence, skill set, and education.[19] The forms also outlined the duties performed by IS members.[20] In April 2016, using information from these forms, Danish authorities identified and arrested five individuals who had fought for IS in Syria and returned home to plot attacks in Europe.[21] The actions of Danish authorities in this case demonstrate potential for CEM to prevent terrorist attacks in the West. To do so, however, the Department of Defense (DOD) must take measures to ensure CEM is not only properly classified and catalogued but also made quickly and readily available to allies and partners.

At this time, the joint force, our allies, and partners have all learned the value of collecting, storing, and cataloguing CEM with the expectation of eventually employing them against VEOs.[22] The idea of using CEM in criminal proceedings is not new. The International Criminal Tribunal for the Former Yugoslavia heard evidence gathered by military police in coordination with the Office of Prosecutor in Srebrenica (1995) and Kosovo (1999). In fact, the evidence accounted for an estimated 65 percent of the total evidence used by the Office of the Prosecutor.[23]

Yet some allies and partner nations continue to struggle in their efforts to introduce CEM into civilian criminal court proceedings. Most of the concern centers on the admissibility of materials captured, collected, or stored by the military from the battlefield.[24]

To alleviate these concerns, the United Nations (UN) in January of this year issued guidelines for the use of battlefield evidence in the criminal prosecution of foreign terrorist fighters.[25] The purpose of these guidelines is to assist UN members in updating and modifying legal frameworks to allow for use of CEM in criminal proceedings. Just as Secretary Esper's memo urges, UN guidelines emphasize the importance for all countries to declassify battlefield evidence and make it readily available for criminal proceedings. The guidelines state:

To ensure the most effective possible use of information in criminal proceedings, States are encouraged to refrain from over-classifying such information. They are also encouraged to develop simplified procedures for the declassification of such materials where they are likely to be used in such proceedings.[26]

The joint force is at the forefront of global efforts to collect, properly classify, declassify, and catalogue CEM so that it can be used as evidence in criminal proceedings against VEOs.[27] Due to these efforts, the FBI has used CEM to identify and arrest terrorists who pose a threat to the U.S. homeland. It is also working to share CEM with its counterparts globally.[28] U.S. attorneys have prosecuted individuals successfully with CEM in the United States, and the Department of Justice has shared this experience with prosecutors worldwide.[29] Yet more work remains to be done. The joint force needs to continue to apply the aforementioned lessons learned from the successful application of CEM to the ongoing fight against violent extremism. This means investing the resources, time, and effort to break down barriers to collection, classification, and sharing of CEM, both domestically and internationally. But it is also the right time to take the lessons

learned from the use of CEM to confront VEOs and apply them to strategic competition.

Applications for Strategic Competition

While the joint force's use of CEM in the fight against VEOs is well documented, CEM also holds unlimited potential for strategic competition. It simply requires creativity in the application. This viewpoint aligns with the 2018 National Defense Strategy, which describes both the central challenge to U.S. national security and the required response as follows:

The central challenge to U.S. prosperity and security is the reemergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.

A long-term strategic competition requires the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military.[30]

When the National Defense Strategy calls on the joint force to be more competitive by looking at its own capabilities relative to these revisionist powers over the long term, it is best understood as part of a wider effort to push back or resist this encroaching authoritarian model that is inimical to U.S. interests. This wider effort includes not only military capabilities and strength but also diplomacy, information, economics, finance, intelligence, and law enforcement. Both the National Defense Strategy and the National Military Strategy emphasize competition *below the level of armed conflict*. They also describe strategic competition as a collective effort with the United States, its allies, and partner nations.[31]

Given this understanding of strategic competition, CEM seems well positioned

as a means to foil any country's use of private military companies (PMCs), paramilitaries, and proxy forces. Some of this is already being done. For example, looking at the U.S. Central Command area of responsibility, the United States recently used CEM recovered by the Armed Forces to highlight Iran's illegal support to Houthi insurgents in Yemen. On November 25, 2019, the USS *Forrest Sherman* legally boarded an unregistered *dhow* (small sailing vessel) in international waters and seized CEM containing unmanned aerial system components, antitank-guided missiles, "near-fully assembled" Iranian surface-to-air missiles, 13,000 blasting caps, and other missile components.[32] A few months later (February 9, 2020), the USS *Normandy* seized a similar cache.[33] In both interdictions, close coordination occurred among DOD, law enforcement, partner nations, and UN weapons inspectors. Indeed, allowing UN inspectors access to this CEM in a timely manner proved critical; the inspectors confirmed and announced to the international community that the weapons were produced by Iran.[34] Secretary of State Mike Pompeo, in turn, has used this CEM in his diplomatic engagements to urge the UN Security Council to extend the arms embargo against Iran.[35]

If CEM can be used effectively in this way against rogue states, such as Iran, it also has applications for strategic competition with revisionist powers. Russia, and its use of PMCs, represents an obvious example. It is well known that the Wagner Group is a Russian PMC led by former Glavnoye Razvedyvatelnoye Upravlenie officer Dmitry Utkin.[36] In June 2017, the Department of Treasury sanctioned Utkin and the Wagner Group for their involvement in Russia's illegal annexation of Crimea.[37] Its fighters directly confronted Special Forces deployed to Syria in February 2018.[38] The Wagner Group also sent weapons along with 1,200 fighters to Libyan General Khalifa Haftar's forces in violation of UN sanctions.[39] In fact, UN sanction monitors recently released details on 122 individuals linked to the Wagner Group who were in Libya to either transfer weapons, provide training to Haftar's forces, or fight.[40]

F/A-18E Super Hornet, assigned to Gunslingers of Strike Fighter Squadron 105, launches from flight deck of USS *Dwight D. Eisenhower*, Arabian Gulf, August 8, 2016, in support of Operation *Inherent Resolve* (U.S. Navy/J. Alexander Delgado)

If the United States, its allies, or partner nations obtained CEM on these individuals, they could substantiate INTERPOL notices and warrants for the paramilitaries' arrests or requests for extradition. Alternatively, CEM used in diplomatic engagements could encourage our allies and partners to enact travel restrictions on the Wagner Group or other relevant Russian PMCs. If successful, these efforts would undermine Russia's ability to send PMCs abroad to bolster authoritarian regimes or otherwise use them as an instrument of foreign policy.

China, and its use of front companies, provides another opportunity to use CEM as part of strategic competition. CEM could be used to defend against Chinese front companies attempting to steal U.S. intellectual property, including military technology. In May 2017, the FBI arrested Shan Shi, a U.S. citizen, and charged him with attempting to steal trade secrets for a Chinese company,

CBM-Future New Material Science and Technology Co., Ltd. (CBMF), and by extension the Chinese government.[41] China does not have the indigenous capability to produce syntactic foam, which is a dual-use technology with applications for deep water oil exploration, as well as Navy submarines and warships. Shan Shi created a front company in Houston and partnered with CBMF to steal this intellectual property.[42] CBMF paid Shan Shi $3.1 million between 2014 and 2017.[43] Using this money, Shan Shi hired employees away from a Houston-based subsidiary of the Swedish company that manufactures syntactic foam, Trelleborg. Shan Shi's new employees obtained spreadsheets from their former colleagues at Trelleborg with details on how to produce syntactic foam and passed this information along to Shan Shi, who then emailed it to CBMF in China.[44] These spreadsheets, emails, and other communications represent just another type of CEM.

Through reciprocal sharing, DOD could use such CEM-derived information to better protect and secure our vital assets and intellectual equities. This information is also an ideal tool for diplomatic engagements, such as highlighting China's efforts to expand its capabilities through the illegal use of front companies or persuading allies and partner nations to enact measures to halt illegal behavior.

These examples illustrate the utility of CEM as an instrument of national power.[45] It has diplomatic, informational, economic, intelligence, law enforcement, and military applications—all of which are named in the National Defense Strategy as elements integral to strategic competition. In order to reach its full potential, however, the declassification and distribution of CEM should be a collective endeavor, including the U.S. Government, allies, and partner nations. Other militaries and law enforcement organizations would need to collect,

properly classify, and share these materials with the United States in a transparent manner, allowing for fulsome exploitation in our counterintelligence efforts, criminal proceedings, and diplomatic engagements.

Final Thoughts

Collected exploitable material provides golden opportunities for collaboration among the joint force, interagency community, allies, and partner nations in the fight against violent extremism. Equally important, the joint force now has a growing body of lessons on the effective utilization of CEM that it can apply in the ongoing competition with revisionist powers and rogue states. Strategic competition requires us to think innovatively, work collaboratively, and utilize every instrument of national power at our disposal. As we begin to think critically through the application of CEM across multidomain operations—domains less developed or yet to be discovered—we must understand that CEM, if applied in this context, provides a myriad of opportunities. Let's not miss them. **JFQ**

- -

Notes

[1] "Honor the Fallen," *Military Times*, available at <https://thefallen.militarytimes.com/army-capt-david-a-boris/3190019>.

[2] Collected exploitable material is all material and/or materiel in the possession of the Department of Defense, regardless of its classification or how it was obtained, that could be exploited in support of DOD and National interests. Examples range from fingerprints and other biometrics to bomb-making materials to internal memos produced and distributed by terrorist leaders. See Mark Esper, "Classification of Materials Captured, Collected, or Handled by the Department of Defense," memorandum, DOD, January 9, 2020; and *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings* (Washington, DC: International Institute for Justice and the Rule of Law, December 2018, available at <https://theiij.org/wp-content/uploads/Non-Binding-Guiding-Principles-on-Use-of-Battlefield-Evidence-EN.pdf>.

[3] *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings.*

[4] See, for example, Charles Faint and Michael Harris, "OPS/INTEL Fusion Feeds the SOF Targeting Process," *Small Wars Journal*, January 31, 2012, available at <https://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process>.

[5] *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings.*

[6] Ibid.

[7] Esper, "Classification of Materials Captured, Collected, or Handled by the Department of Defense."

[8] Ibid.

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

[10] Central Intelligence Agency, "CIA Releases Nearly 470,000 Additional Files Recovered in May 2011 Raid on Usama Bin Ladin's Compound," press release and statements, November 1, 2017, available at <https://www.cia.gov/news-information/press-releases-statements/2017-press-releases-statements/cia-releases-additional-files-recovered-in-ubl-compound-raid.html>. See also Combating Terrorism Center at West Point, "Harmony Program," available at <https://ctc.usma.edu/harmony-program/>; Office of the Director of National Intelligence, "Bin Laden's Bookshelf," available at <https://www.dni.gov/index.php/features/bin-laden-s-bookshelf>; Central Intelligence Agency, "November 2017 Release of Abbottabad Compound Material," available at <https://www.cia.gov/library/abbottabad-compound/index.html>.

[11] The term *external operations* refers to terrorist attacks that take place outside a violent extremist organization's safe haven or primary areas of operation. It is distinct from the more traditional term *international terrorism*. For example, al Qaeda affiliate Jemaah Islamiyyah executed an attack against the Australian embassy in Jakarta, Indonesia, in September 2004. This attack falls into the category of international terrorism because the target was the Australian embassy. However, it is not considered an external operation because Islamiyyah is based in Indonesia. Al Qaeda leaders focused their external operations on the so-called far enemy or Western countries.

[12] Office of Public Affairs, Department of Justice, "Al Qaeda Operative Convicted for Role in International Terrorism Plot Targeting the United States and Europe," press release, March 4, 2015, available at <https://www.justice.gov/opa/pr/al-qaeda-operative-convicted-role-international-terrorism-plot-targeting-united-states-and>.

[13] *United States v. Naseer*, 16-373-cr (U.S. Court of Appeals for the Second Circuit, August 20, 2019), available at <www.leagle.com/decision/infco20190820084>.

[14] Office of Public Affairs, Department of Justice, "Man Sentenced for Terrorism-Related Crimes," press release, November 7, 2018, available at <https://www.justice.gov/opa/pr/syrian-man-sentenced-terrorism-related-crimes>. See also Morgan Loew, "Fingerprints Led FBI to Notorious IED Maker," CBS News, November 9, 2018, available at <www.azfamily.com/news/investigations/cbs_5_investigates/fingerprints-led-fbi-to-notorious-ied-maker/article_3be84fc0-e466-11e8-abb0-078163cc8e32.html>.

[15] Ibid. See also U.S. Attorney's Office, Phoenix, Arizona, "Defendant Extradited to the United States to Face Terrorism Charges," press release, August 28, 2014, available at <https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/defendant-extradited-to-u.s.-to-face-terrorism-charges>.

[16] "Turkey Extradites ISIS-Linked Syrian to U.S. on Terror Charges," *Daily Sabah* (Istanbul), September 2, 2014, available at <www.dailysabah.com/mideast/2014/09/02/turkey-extradites-isislinked-syrian-to-us-on-terror-charges>. Other examples also exist. In 2011 in *United States v. Alwan*, the FBI's Terrorist Explosive Device Analytic Center (TEDAC) matched the fingerprints from an improvised explosive device produced in Iraq (around 2005) to a man living in Kentucky. TEDAC has received over 100,000 IED submissions from over 50 countries. See *Non-Binding Guiding Principles on the Use of Battlefield Evidence in Civilian Criminal Proceedings.*

[17] Amandine Scherrer, ed., *The Return of Foreign Fighters to EU Soil, Ex-Post Evaluation* (Brussels: European Parliament Research Service, May 2018), 49, available at <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)621811>; Arthur Martin, Ian Drury, and Martin Robinson, "ISIS Staff List Is Leaked: Names and Family Details of 22,000 Jihadis Revealed in Cache of Application Forms Complete with References (and Next of Kin)," *Daily Mail*, March 10, 2016, available at <https://www.dailymail.co.uk/news/article-3484702/Names-family-details-22-000-jihadis-revealed-huge-cache-leaked-ISIS-HR-forms.html>.

[18] Ibid.

[19] Martin, Drury, and Robinson, "ISIS Staff List Is Leaked."

[20] Europol, *European Union Terrorism Situation and Trend Report 2017* (Brussels: European Agency for Law Enforcement Cooperation, June 15, 2017), 19, available at <https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017>.

[21] Vickiie Oliphant, "Terror Warning: ISIS Files Reveal Danish Recruiters Who 'Plotted Attack' Links to UK," *Express Online*, April 18, 2016, available at <https://www.express.

co.uk/news/world/662217/ISIS-files-Danish-recruiters-linked-to-UK>.

22 Sajid Javid, "UK Nationals Returning from Syria," presentation before the House of Commons, February 18, 2019, available at <www.theyworkforyou.com/debates/?id=2019-02-18c.1193.0>.

23 Bibi van Ginkel and Christophe Paulussen, *The Role of the Military in Securing Suspects and Evidence in the Prosecution of Terrorism Cases Before Civilian Courts: Legal and Practical Challenges*, ICCT Research Paper (The Hague: International Centre for Counter-Terrorism, May 2015), available at <https://icct.nl/wp-content/uploads/2015/04/ICCT-Van-Ginkel-Paulussen-The-Role-Of-The-Military-In-Securing-Suspects-And-Evidence-In-The-Prosecution-Of-Terrorism-Cases-Before-Civilian-Courts.pdf>.

24 Ibid.

25 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), *Guidelines to Facilitate the Use and Admissibility as Evidence in National Criminal Courts of Information Collected, Handled, Preserved, and Shared by the Military to Prosecute Terrorist Offences* (New York: CTED, January 2020), available at <https://www.un.org/sc/ctc/wp-content/uploads/2020/01/Battlefield_Evidence_Final.pdf>.

26 Ibid.

27 While this article focuses on efforts to bring battlefield evidence into civilian courtrooms to minimize threats against the U.S. homeland and the West, it is worth noting that the joint force also has been very much invested in using CEM to mitigate the devastating impact of IEDs on Servicemembers. CEM recovered from a blast site by trained experts (such as explosive ordnance device teams) has enabled the joint force to counter future IED strikes by attacking the insurgent network(s). This has been accomplished by exploiting the acquired CEM and analyzing its derived information and intelligence for biometrics (fingerprints and DNA), the origin of its components, or its explosive composition (military grade, commercial, or homemade), to name a few. Numerous organizations have been involved in these efforts over the past 20 years, including the Joint Improvised Explosive Devise Defeat Organization and the Joint Improvised-Threat Defeat Organization (now called the Defense Threat Reduction Agencies' Directorate of Operations and Integration).

28 Europol, *European Union Terrorism Situation and Trend Report 2017*; Scherrer, *The Return of Foreign Fighters to EU Soil*, 49; Europol, *European Union Terrorism Situation and Trend Report 2019* (Brussels: European Agency for Law Enforcement Cooperation, June 27, 2019), available at <https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat>; Nathan A. Sales, "After the Caliphate: A New Global Approach to Defeating ISIS,"

remarks by the Coordinator for Counterterrorism at the Brookings Institution, Washington DC, April 30, 2019, available at <https://www.state.gov/after-the-caliphate-a-new-global-approach-to-defeating-isis/>.

29 Europol, *European Union Terrorism Situation and Trend Report 2017*; *Scherrer, The Return of Foreign Fighters to EU Soil*, 49; Europol, *European Union Terrorism Situation and Trend Report 2019*; Sales, "After the Caliphate.".

30 *Summary of the 2018 National Defense Strategy of the United States of America*, 2, 4. Emphasis in original.

31 Ibid. See also *Description of the National Military Strategy 2018* (Washington, DC: The Joint Staff, 2018), available at <https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf>.

32 U.S. Central Command, "U.S. Dhow Interdictions," public affairs release, February 19, 2020, available at <https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/2087998/us-dhow-interdictions/>.

33 Ibid.

34 Ibid.

35 "Pompeo Says U.S. Seized Iranian Weapons on Way to Houthi Rebels In Yemen," Reuters, July 8, 2020, available at <www.reuters.com/article/us-usa-iran-pompeo/pompeo-says-un-arms-embargo-on-iran-must-be-extended-to-prevent-further-regional-conflict-idUSKBN2492AV>.

36 Department of the Treasury, "Treasury Designates Individuals and Entities Involved in the Ongoing Conflict in Ukraine," press release, June 20, 2017, available at <https://www.treasury.gov/press-center/press-releases/Pages/sm0114.aspx>.

37 Ibid.

38 Thomas Gibbins-Neff, "How a 4-Hour Battle Unfolded Between Russian Mercenaries and U.S. Commandos in Syria," *New York Times*, May 24, 2018, available at <www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html>.

39 "UN Monitors Say Mercenaries from Russia's Wagner Group Fighting in Libya," Radio Free Europe, May 7, 2020, available at <https://www.rferl.org/a/wagner-un-russia-libya/30598355.html>.

40 Ibid.

41 Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets," press release, July 29, 2019, available at <https://www.justice.gov/opa/pr/texas-man-convicted-conspiracy-commit-theft-trade-secrets>; Meagan Flynn, "Houston Area Engineers Accused of Stealing Trade Secrets to Benefit China's Military," *Houston Press*, May 25, 2017, available at <www.houstonpress.com/news/six-engineers-in-houston-charged-in-plot-to-steal-trade-secrets-to-benefit-china-9467242>.

42 Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets"; Flynn, "Houston." See also Office of Public Affairs, Department of Justice, "Two Businessmen Charged with Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company," press release, April 27, 2018, available at <https://www.justice.gov/opa/pr/two-businessmen-charged-conspiring-commit-economic-espionage-benefit-chinese-manufacturing>; Spencer Hsu, "Houston Businessman Convicted of Conspiring to Steal Trade Secrets, Acquitted of Economic Espionage for China," *Washington Post*, July 29, 2019, available at <www.washingtonpost.com/local/legal-issues/houston-businessman-convicted-of-conspiring-to-steal-trade-secrets-acquitted-of-economic-espionage-for-china/2019/07/29/92418df2-b245-11e9-8f6c-7828e68cb15f_story.html>; *United States v. Shan Shi*, 2019 U.S. Dist. Lexis 218100 (United States District Court for the District of Columbia, December 17, 2019, Filed), available at <www.lexislegalnews.com/articles/46649/judge-rejects-acquittal-bid-by-defendant-in-trade-secret-theft-suit>.

43 Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets"; Flynn, "Houston." See also Office of Public Affairs, Department of Justice, "Two Businessmen Charged with Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company"; Hsu, "Houston Businessman Convicted of Conspiring to Steal Trade Secrets, Acquitted of Economic Espionage for China"; *United States v. Shan Shi*.

44 Office of Public Affairs, Department of Justice, "Texas Man Convicted of Conspiracy to Commit Theft of Trade Secrets"; Flynn, "Houston." See also Office of Public Affairs, Department of Justice, "Two Businessmen Charged with Conspiring to Commit Economic Espionage for Benefit of Chinese Manufacturing Company"; Hsu, "Houston Businessman Convicted of Conspiring to Steal Trade Secrets, Acquitted of Economic Espionage for China"; *United States v. Shan Shi*.

45 DOD defines *instruments of national power* thus: "All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational and military." See Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, July 12, 2017), available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2019-02-11-174350-967>.

NDU Press Congratulates the Winners of the 2020 Essay Competitions

NDU Press virtually hosted the final round of judging in May 2020, during which 26 faculty judges from 14 participating professional military education (PME) institutions selected the best entries in each category. There were 72 submissions in this year's three categories. First Place winners in each of the three categories appear in the following pages.

Secretary of Defense National Security Essay Competition

The 14th 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 (tie)
Lieutenant Colonel Roderick K. Butz, USAF
U.S. Army War College
"Beneath the Crosshairs: Remotely Piloted Airstrikes as a Foreign Policy Tool"

First Place (tie)
Kaleb J. Redden, Office of the Secretary of Defense
National War College
"Competition Is What States Make of It: A U.S. Strategy Toward China"

Second Place
Kyle Richardson, Department of State
National War College
"Indonesia: Lessons for the U.S.-China Geo-Economic Competition"

Third Place
Lieutenant Colonel Eric V.M. Kreitz, USA
U.S. Army War College
"Re-Emerging Russian Influence in Latin America and U.S. Foreign Policy Response"

Chairman of the Joint Chiefs of Staff Strategic Essay Competition

This annual competition, in its 39th year in 2020, 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
Lieutenant Colonel Jeremy McKissack, USAFR
Air War College
"Pardon the Paradox: Making Sense of President Trump's Interventions in Military Justice"

Second Place
Lieutenant Colonel Matthew Kendrick Mulvey, USMC
U.S. Naval War College (Senior)
"Helping Hanoi Keep the Dragon at Bay in the South China Sea"

Third Place
Amy C.F. Carlon, Department of State
Eisenhower School for National Security and Resource Strategy
"Diplomatic Engagement on Missile Defense Amidst Great Power Competition"

Strategy Article

First Place
Colonel Mark M. Zais, USA
U.S. Army War College
"Artificial Intelligence: A Decisionmaking Technology"

Second Place
Lieutenant Colonel Kukunaokala (Kuna) Mendonca, ARNG
U.S. Army War College
"Cybersecurity Initiatives in the National Guard: Opportunities and Challenges"

Third Place
Lieutenant Colonel Jeremy McKissack, USAFR
Air War College
"First Among Equals: Diplomacy as America's Primary Instrument of Power"

Joint Force Quarterly Maerz Awards

In its 5th year, the *JFQ* Maerz Awards, chosen by the staff of NDU Press, recognize the most influential articles from the previous year's four issues. Six outstanding articles were chosen for the Maerz Awards, named in honor of Mr. George C. Maerz, former writer-editor of NDU Press.

Forum
Glenda Jakubowski
"What's Not to Like? Social Media as Information Operations Force Multiplier," *JFQ* 94 (3rd Quarter 2019)

JPME Today
Dale C. Eikmeier
"Simplicity: A Tool for Working with Complexity and Chaos," *JFQ* 92 (1st Quarter 2019)

Commentary
Jeffery Zust and Stephen Krauss
"Force Protection from Moral Injury: Three Objectives for Military Leaders," *JFQ* 92 (1st Quarter 2019)

Features
Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden
"Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *JFQ* 92 (1st Quarter 2019)

Recall
John K. DiEugenio and Aubry J. Eaton
"Flanking the Crater," *JFQ* 94 (3rd Quarter 2019)

Joint Doctrine
J. Mark Berwanger
"Fire for Effect: The Evolution of Joint Fires," *JFQ* 93 (2nd Quarter 2019)

Distinguished Judges

Twenty-six senior faculty members from the 14 participating PME institutions took time out of their busy schedules (and online teaching duties) to serve as judges for this year's competitions. Their personal dedication and professional excellence ensured strong and credible competitions.

The judges were Joseph L. Billingsley, College of Information and Cyberspace; Brandy Lyn Brown, Marine Corps University; Mark A. Bucknam, National War College; Dr. Charles Chadbourne, U.S. Naval War College; Dr. James Chen, College of Information and Cyberspace; Dr. Benjamin "Frank" Cooling, Eisenhower School for National Security and Resource Strategy; Dr. Armando DeLeon, Air University eSchool of Graduate PME; Dr. Richard L. DiNardo, Marine Corps Staff College; Dr. Peter Eltsov, College of International Security Affairs; Dr. Jack Godwin, NDU Press; Dr. Todd Holm, Marine Corps University; Dr. C.J. Horn, Air Force Cyber College; Dr. James D. Kiras, School of Advanced Air and Space Studies; Captain Bill Marlowe, USN (Ret.), Joint Forces Staff College; Dr. Brian McNeil, Air War College; Dr. Larry D. Miller, U.S. Army War College; Dr. Kristin Mulready-Stone, U.S. Naval War College; Dr. Jaimie Orr, National War College; Dr. Nicholas M. Sambaluk, Air University eSchool of Graduate PME; Dr. Jesse P. Samluk, National Intelligence University; Dr. Nicholas E. Sarantakes, U.S. Naval War College; Dr. Naunihal Singh, U.S. Naval War College; Dr. Paul Springer, Air Command and Staff College; Dr. Jeff Turner, Joint Forces Staff College; Dr. David A. Wigmore, College of International Security Affairs; and Dr. Elizabeth D. Woodward, Air War College.

Sailors signal to MH-60S Sea Hawk helicopter attached to Golden Falcons of Helicopter Sea Combat Squadron 12 as it hovers over flight deck of USS *McCampbell* during visit, board, search, and seizure training exercise, South China Sea, July 22, 2016 (U.S. Navy/Elesia K. Patten)

Competition Is What States Make of It: A U.S. Strategy Toward China

By Kaleb J. Redden

They have transformed a poor society by an economic miracle to become now the second-largest economy in the world. . . . They have followed the American lead in putting people in space and shooting down satellites with missiles. Theirs is a culture 4,000 years old with 1.3 billion people, many of great talent. . . . How could they not aspire to be number 1 in Asia, and in time the world? . . . It is China's intention to be the greatest power in the world.

—Lee Quan Yew, former prime minister of Singapore[1]

Kaleb J. Redden wrote this essay while a student at the National War College. It tied for first place in the 2020 Secretary of Defense National Security Essay Competition.

China today represents the "most consequential long-term challenge we face as a nation."[2] While many actors and trends present challenges to U.S. interests, only China has the potential to challenge the United States across so many aspects of national power—to challenge its economic influence and technological lead in key sectors, to challenge its military in scenarios in which it has long held dominance or assumed sanctuary, or to present an alternative governance model that undermines the norms and

values that the United States has sought to preserve at home and promote abroad.[3] To be clear, China faces many headwinds that may inhibit its rise.[4] Yet China has signaled ambitions to be a dominant global power; its economic trajectory, if it continues, would provide significant means to pursue its aims.[5] As a result, today China alone can contend with the United States for hegemony within a region and has the potential to mount a serious challenge to the U.S. ability to shape the character of the international system.[6]

This article provides a U.S. strategy for this challenge.[7] It begins from a view that the United States benefits from its leading position in the international order of the past 75 years.[8] It embraces the diagnosis of our current national strategies that U.S.-China relations have become more competitive, but diverges on some of the approaches it recommends to succeed in that competition. It posits that, while the primacy the United States once enjoyed may no longer be attainable, the United States still maintains the wherewithal to prevent Chinese hegemony in Asia and to sustain its leading role in shaping the character and direction of global affairs—and that the U.S. political aim should be to do so.[9] It argues that the United States can achieve this aim by reinforcing deterrence in Asia, building a balancing coalition to check China's rise, and bolstering domestic strengths to extend U.S. influence and sustain the international order until China either moderates its ambitions or suffers setbacks. In other words, the United States should not panic, but it must focus.

The Strategic Context: International and Domestic

China's Trajectory, Ambitions, and Strategy. Over the past 40 years, China has witnessed an unprecedented economic transformation, rising from a poor, isolated state to become the world's second largest economy, largest merchandise exporter, second largest destination of foreign direct investment, and largest manufacturer.[10] Throughout most of that time, China's leaders were mindful of Deng Xiaoping's dictate to "hide your

capabilities and bide your time," creating space for its rise while allowing the world to believe it might become a "responsible stakeholder" in the international system.[11]

The arrival of President Xi Jinping in 2012, however, ushered in a new era of Chinese confidence and assertiveness. China is hiding its capabilities no longer; it portrays itself as a world leader and casts the United States as retreating from the global stage. Under Xi's leadership, China has sought to reorient global economic corridors through its Belt and Road Initiative (BRI), militarized extraterritorial claims in the South China Sea, undertaken a massive military modernization campaign, and set goals to dominate key technology sectors by 2025. Perhaps most significant, Xi's articulation of a new "Chinese Dream" set ambitious national objectives that, according to some interpretations, aim to supplant the United States economically, militarily, and culturally by 2049.[12] Ultimately, China seeks to achieve dominant influence in its near abroad and to displace the United States from its historical role as the de facto leader of the international order so that it can reshape that order to its preferences.[13]

China's strategy to achieve these aims has increasingly come into focus. It seeks to increase its leverage through trade and economic tradecraft so that nations, corporations, and organizations are reticent to contest or even criticize China's activities; increase its military capabilities to deter U.S. military intervention in Asia; weaken the U.S. alliance system, particularly in Asia; erode confidence in U.S. credibility and staying power; cast doubt on the U.S. economic and political model; and increasingly present itself as a leader in global institutions and in the eyes of the world.[14] It seeks to do so while avoiding a conflict with the United States, but it is increasingly confident of its prospects should one emerge.[15] A successful U.S. theory of victory must be designed to defeat this Chinese theory of victory.[16]

U.S. Domestic Context: Advantages and Atrophy. As these dynamics have become more evident, a consensus has emerged in Washington that the United States must move aggressively to stop

this erosion.[17] Donald Trump's National Security Strategy may have given official voice to a more competitive U.S.-China relationship, but there is a growing bipartisan consensus on the gravity of this issue, which is rare in Washington today.

Despite this sense that its dominance is eroding, the United States today still enjoys a number of enduring strengths that China lacks. These include an unparalleled alliance network,[18] unrivaled military power projection capabilities, a highly efficient and innovative economy,[19] systemic fiscal and economic advantages,[20] abundant natural resources and energy reserves,[21] a comparatively uncontested near abroad,[22] and an open society and comparatively transparent government with greater legitimacy, elite educational institutions,[23] more favorable demographics,[24] and a historic position as de facto leader of the international order.[25] And China faces significant challenges often overlooked in narratives of its inevitable rise, including widespread corruption, poor health care, an aging population, and many others.[26] In short, China is not preordained to supplant the United States globally.[27]

Yet the United States has frittered away many of its advantages. At home, it has underfunded education and infrastructure, insufficiently prioritized research and development, abandoned immigration policies that have underwritten U.S. economic competitiveness, and allowed other domestic strengths to wither.[28] It is experiencing new levels of political polarization and national debt that leave it less able to stem this atrophy or respond to other crises. And abroad, an "America First" foreign policy has put strains on U.S. alliances,[29] undercut U.S. attractiveness,[30] created a vacuum in international institutions that China has moved to fill,[31] and, most important, left the world less confident of U.S. leadership.[32]

Moreover, while Washington has become seized with this problem, it is unclear that the American public has done so. Some polling suggests that the public is less focused on China than political elites.[33] The public already expects a level of services incommensurate with taxation;

F-35B Lightning II fighter aircraft with Marine Medium Tiltrotor Squadron 265 (Reinforced), 31st Marine Expeditionary Unit, prepares to take off from flight deck of amphibious assault ship USS *America*, South China Sea, April 18, 2020 (U.S. Marine Corps/Isaac Cantrell)

the United States was running nearly trillion-dollar deficits even before the coronavirus pandemic. To put it simply, the public does not appear prepared for the commitment that a long-term U.S.-China competition might entail. Whether the United States will sustain its advantages is therefore unclear; this strategy must demonstrate why the public should be willing to support doing so.

U.S. National Interests and How China Threatens Them

The United States must weigh Chinese actions by the degree to which they threaten its national interests. While formulations for national interests have varied, they are typically variants of security, prosperity, and the values we seek to preserve at home and promote abroad.[34] China poses significant challenges to each.

Protecting U.S. Security. The United States remains the world's preeminent military, with unrivaled global power. But *regional* balances of power are what matter vis-à-vis China—because the potential flashpoints today are proximate to China, and Beijing has been investing in capabilities specifically designed to challenge Washington in such scenarios.[35] Unless the United States is postured to blunt Chinese aggression initially, it faces the unwelcome choice of either seeking to roll back Beijing's advances or backing down. With the former come risks of escalation against a nuclear power; with the latter comes weakened U.S. credibility and norms against nonaggression.[36] Put simply, U.S. military deterrence in Asia, which numerous allies trust for their own security, is eroding, and the risk of conflict is rising as a result.

Long-term trends are also bleak. The United States has spent the past two decades focused on counterterrorism and counterinsurgency—investing in legacy systems and consuming readiness as quickly as possible. As a result, China today rivals the United States in key technologies such as artificial intelligence, quantum computing, and hypersonics.[37] It appears capable of using cyber capabilities to hold at-risk critical infrastructure, penetrating military networks critical to our power projection, and engaging in social manipulation to cripple the public's will.[38] It is eroding U.S. advantages one by one, often by stealing technology that required billions of dollars and years to develop.[39] Put simply, the character of warfare is changing, and China has done more to prepare for it.

Promoting U.S. Prosperity. China has eclipsed the United States as the primary trading partner for nearly all the world's nations, reversing a dominant U.S. position of only 20 years ago.[40] The

International Monetary Fund estimates that if China achieves its 2049 goals, its economy would be three times that of the United States.[41] While scholars rightly point out that China must also provide for more than four times the U.S. population, this sheer economic heft would give China enormous benefits of scale as well as significant leverage in almost any bilateral relationship.

To grow and sustain these advantages, the goals of "Made in China 2025" make clear China's intent to dominate key technology areas it believes are essential to future growth—a goal that implies displacing U.S. leadership in many cases.[42] To do so, it restricts foreign companies' access to Chinese markets, supports state-owned enterprises, forces companies to share intellectual property (IP), and steals IP it cannot otherwise obtain. The Commission on Intellectual Property Theft estimates that cyber theft costs the United States between $180 billion and $540 billion annually—the equivalent of 1 to 3 percent of U.S. gross domestic product.[43] Intangible assets such as IP represent 80 percent of the value of the Standard and Poor's 500 by some estimates, so vulnerability to such attacks is consequential for both economic prosperity and national security.[44]

Moreover, China reinforces this leverage with tools of economic statecraft, most notably its Belt and Road Initiative. Most estimates suggest China plans to spend more than $1 trillion globally under BRI, which will reorient global trade corridors toward China.[45] As part of this effort, China engages in predatory lending—simultaneously linking these nations to China's economic system, generating coercive leverage, and undercutting international norms.[46] The United States has no compelling alternative to these offerings.

As a result, even as states become more wary of China's motives, its economic leverage provides a powerful tool to promote its preferences and undermine U.S. influence. At least one analysis of Asian power trends now rates China as the most diplomatically influential nation in Asia.[47] In Latin America, China is using this leverage to pressure states to drop diplomatic recognition of Taiwan.[48] In Europe, U.S. efforts to convince nations not to allow Huawei to build 5G networks have fallen flat.[49] Nations increasingly want U.S. security but still want Chinese economic benefits, and they try to avoid being forced to choose.[50]

Advancing U.S. Values and Influence. China's governance model presents the most credible alternative model to Western democracy since the fall of the Soviet Union. Chinese citizens cede political freedom in exchange for economic gain,[51] allowing the Chinese Communist Party to create an unparalleled surveillance state.[52] Xi has arrested thousands of activists, expelled foreign journalists, and worked to suppress protests in Hong Kong. Most egregiously, China has detained more than 1 million Uighurs, Kazakhs, and other Muslim minorities in "reeducation camps," with torture and forced labor being reported.[53] U.S. experts have comforted themselves with the thought that China's model lacks foreign appeal.[54] Yet recent behavior suggests China increasingly sees its model as something it should export.[55] If it spreads, not only will millions of people be less free, but current norms that guide nation-state behavior will be at risk as well. Such a future presents a challenge to our values and portends a darker world where unrest and conflict are more common—potentially undercutting long-term global stability as well.[56]

Desired Ends, Theory of Victory, and Assumptions

The United States must decide if it wishes to confront this challenge or seek some form of accommodation with China. This strategy argues that the United States is unlikely to reach any accommodation that would be sufficient to protect its own interests yet satisfy Beijing over the long term.[57] China's ambitions are at odds with core tenets of U.S. foreign policy: preventing a foreign hegemon in Asia, supporting allies and partners who feel threatened by China's rise, and reluctantly conceding regional spheres of influence in which China would dictate the norms of behavior. It is always possible that China's aims are less ambitious. U.S. strategy, however, must account for the possibility that they are not.

As a result, the U.S. political aim should be to deny China regional hegemony and to sustain the leading role of the United States in shaping the character and direction of global affairs. The United States still maintains the wherewithal to do so today, even if it is unlikely to regain the primacy it enjoyed following the collapse of the Soviet Union. To do so, this strategy offers a theory of victory designed to counter China's strategy: the United States must reinforce deterrence in Asia to mitigate vulnerabilities today, build a balancing coalition to check China's rise, and bolster U.S. domestic strengths to extend American influence and sustain the international order until China either moderates its ambitions or suffers setbacks.

Given's China's breathtaking rise, we should be clear about the plausible mechanisms for this theory of victory to work. Even as some trends appear significantly in China's favor, this theory could work by buying time and signaling U.S. commitment that allows states to form a balancing coalition against China,[58] buying time for China's domestic constraints to work against it, either through economic stagnation or more far-reaching domestic upheaval,[59] or by simply sustaining U.S. advantages that prove more pronounced than declinists predict.[60] Competing with rather than accommodating China is also advisable even if none of these futures transpires, because even if its current position in the international order is not viable indefinitely, the United States benefits from sustaining it for as long as possible.

This approach, however, relies on a number of assumptions. If any of these proved invalid, it would require revisiting the strategy. Key assumptions include the following:

- The current international order remains attractive to most nations.[61]
- The United States can convince nations to balance against China.[62]

- China's leaders can adjust policy without imperiling regime stability.[63]
- U.S. actions designed to deter Chinese behavior will in fact improve deterrence, not drive an escalatory response.[64]
- Other threats (for example, Russia) will not alter Chinese behavior significantly or align with one another in ways that significantly increase the threat they pose to U.S. interests.
- The U.S. public will support increased investments necessary to execute this strategy.
- Access to Asia's economy is necessary for U.S. prosperity.
- U.S. economic fundamentals (for instance, the dollar as a safe-haven currency) will not shift significantly.
- Relative Chinese and U.S. economic and military trends are such that we may see a "period of acute danger" rather than China's inexorable rise.[65]

Strategic Objectives

This strategy articulates four key objectives that, taken together, are designed to pursue this theory of victory and achieve the strategy's political aim:

- Bolster conventional deterrence in Asia. This step includes both near-term measures to deter Chinese aggression and longer term efforts to sustain the U.S. military edge.
- Build a balancing coalition to check China's rise. To do so, the United States must reinvest in its alliances, restore perceptions of U.S. leadership and support for the international order, level the economic playing field with China by pursuing reciprocal trade rules and by building alternatives to BRI, and undertake a messaging campaign to expose the gap between China's narratives and its behavior.
- Restore the sources of long-term U.S. domestic strength. This step includes investments at home to revitalize our economy and society as well as discipline to prioritize resources to meet the challenge that China poses.

- Pursue "principled engagement." Even as we take the steps above, we should look to cooperate with China where our interests align to provide ballast for the relationship as competition intensifies, improve crisis stability, and make progress where possible on global issues.

These objectives are designed to be mutually reinforcing and to produce cumulative effects. They could be pursued in parallel, though some of them may necessarily allow for faster action than others.

What follows is a series of "objective instrument packages" that tie the objectives above to specific ways and means. An overarching strategy for China could not possibly account for every specific action the United States should take given the breadth and complexity of U.S.-China competition today. These objectives, however, provide key elements that should guide the U.S. approach and could also inform more detailed Department of Defense (DOD) strategies.

Objective 1: Bolster Conventional Deterrence in Asia. The United States must begin by launching a campaign to bolster conventional deterrence in Asia. The National Defense Strategy provides useful direction on this issue. More needs to be done to implement it, however, and some of its prescriptions are incomplete.

Ensuring there is no opportunity for Chinese aggression is important because it shores up an acute vulnerability. It is also a useful first step because other nations expect it, and because it is a bedrock requirement for stability on which other initiatives can ride: with it as a bulwark, we can work to rebuild other nations' confidence in the United States and over time enable them to stand with us on economic and diplomatic matters.

This effort must begin with urgently needed investments and changes to capabilities and force posture.[66] To do so, DOD must prioritize acquisition of more lethal and survivable platforms (advanced munitions; more resilient command, control, communications, computers, intelligence, surveillance, and

reconnaissance), increase U.S. regional force posture and improve its combat credibility (more dispersed and resilient basing),[67] develop new operational concepts for defeating Chinese aggression without the all-domain dominance to which U.S. forces have become accustomed since the Gulf War,[68] and identify critical infrastructure for U.S. power projection and develop cyber protection campaigns given the importance of U.S.-based surge forces for most Indo-Pacific contingencies.[69]

Deterrence is not simply about capabilities; it is also about resolve. While the decision to use force will always be made by the President at the time, the United States must be prepared to fight in those situations where we seek to deter.[70] To that end, as the United States updates its posture and deploys more advanced capabilities, it should undertake a calibrated messaging campaign to Beijing that signals both our defensive intentions and our unequivocal preparedness to act in the event of significant Chinese aggression against U.S. forces or allies.

The second element of this objective is longer term efforts to sustain our military edge. The National Defense Strategy emphasizes creating a more lethal force but gives little guidance on the relative emphasis on known capabilities versus long-term disruptive technology. As a result, the military departments' proclivity toward familiar platforms means that DOD has focused more on near-term lethality. DOD has made notable steps in increasing its research and development (R&D) spending,[71] but much of this funding has focused on evolutionary rather than revolutionary gains.[72] To address this issue, DOD should first sustain its R&D funding increases—even at the expense of force structure or additional readiness—and significantly increase investment in long-term R&D on key technology areas such as artificial intelligence, hypersonics, space systems, and quantum computing. Second, because R&D spending is increasingly driven by the private sector, DOD must not only increase spending but also undertake acquisition reforms to speed up commercial technology integration, experimentation,

From left, USS *Germantown*, USNS *John Ericsson*, USS *Antietam*, USS *Ronald Reagan*, USS *America*, USS *Shiloh*, USS *New Orleans*, and USS *Comstock* break away from formation in support of Valiant Shield 2020, Philippine Sea, September 25, 2020 (U.S. Navy/Oswald Felix, Jr.)

and fielding.[73] And third, DOD, working with the Departments of State and Commerce, should continue to drive export control reforms—improving our ability to protect technological crown jewels while making it easier to share noncontroversial technology with allies.

Objective 2: Build a Balancing Coalition to Check China's Rise. If China's trajectory continues, building a balancing coalition of states to sustain a favorable balance of power is the most plausible mechanism to counter China's rise. Credible deterrence is crucial, but convincing nations to take this step would also require the United States to strengthen frayed bonds among its allies and partners, reestablish perceptions of U.S. leadership and commitment to the international order, develop alternatives to Chinese economic statecraft, and expose China's malign behavior.

Strengthening U.S. Alliances and Partnerships. The U.S. alliance network is a substantial advantage that China lacks but seeks to undermine. Yet the United States risks taking this advantage for granted. It is no secret that many allies have chafed at President Trump's "America First" rhetoric and demands for increased burden-sharing at a time when many allies face economic challenges and have just spent the past two decades supporting the United States in Iraq and Afghanistan. In some quarters, these relationships already appear to be fraying. One need look no further than the Philippines' termination of the Visiting Forces Agreement, the British decision on Huawei, or European nations seeking to create an alternative to the Society for Worldwide Interbank Financial Telecommunication.[74] Yet on balance, the United States still has substantial leverage today, is seen by

many nations as their de facto security guarantor, and is still trusted more than China—advantages we can leverage but must shore up.[75]

First, the United States must simply act in word and deed as if its alliance and partner relationships matter. Washington should begin by turning down the rhetoric on burden-sharing in both Europe and Asia and moderating its aims in particular negotiations such as the Special Measures Agreement with the Republic of Korea. It should consult with partners before making significant foreign policy decisions (for example, closing U.S. borders without consulting allies was a self-inflicted wound in the initial coronavirus response). And it should simply be more present and dependable diplomatically (for example, President Trump has attended only two of eight summits in Asia during his tenure).

F/A-18E Super Hornet, attached to Eagles of Strike Fighter Squadron 115, launches from flight deck of Navy's only forward-deployed aircraft carrier USS *Ronald Reagan*, Philippine Sea, August 31, 2020 (U.S. Navy/Erica Bechard)

The United States should couple this shift in diplomatic posture with increased assistance and collaboration. For instance, it could increase and reprioritize its security assistance programs—providing more assistance to states vulnerable to Chinese coercion while also being more direct about specific capabilities—with the goal of incentivizing vulnerable states to become "porcupines" that are difficult to invade and more able to withstand Chinese harassment. DOD should also develop analytic processes to optimize defense capability mixes among sophisticated allied militaries (for example, Japan and Australia) to improve complementary capabilities given new operational concepts. And it should seek to persuade Quadrilateral Security Dialogue nations (Japan, Australia, India, and the United States) and key European allies to increasingly join such activities as Freedom of Navigation exercises, which signal joint resolve and bind these nations to us.

Reestablishing Perceptions of U.S. Leadership and Commitment to the International Order. Additionally, the United States should seek to reestablish the perception among nations that it remains committed to and prepared to play a leading role in the international order. For 70 years, the United States has widely been seen as the creator, defender, and de facto leader of the order. Yet as the Trump administration has criticized U.S. involvement in aspects of the order, China has sought to step into this vacuum, portraying itself as a global leader as the United States retreats.[76]

To shift this trend, the United States must begin by demonstrating a renewed commitment to international institutions. It must increase U.S. participation in international standard-setting bodies, many of which draw few headlines but do critical work. China has been increasingly staffing these agencies, then using its positions to insert official references to BRI or Xi Jinping's "Community with a Shared Future for Mankind" and shaping norms like the "Responsibility to Protect" to accommodate China's sovereignty concerns.[77] The United States must also make its contributions for United Nations funding on time and without coercive demands. Nations have not forgotten the years of demands for zero real growth that Washington placed on these organizations. Many will view President Trump's recent decision to withhold funding for the World Health Organization as a politically motivated attempt to shift blame for the coronavirus pandemic. And the United States must reconsider its posture in certain situations to avoid appearing obstructionist. For example, the United States recently blocked the appointment of judges to the World Trade Organization's dispute resolution court until the court could finally no longer reach a quorum,[78] ending 27 years of enforcement.[79] Some 67 nations petitioned the United States to shift its position. When Washington refused, the European Union worked with other nations—including China—to create a workaround.[80] China looks like a constructive actor here, but the United States does not.

Second, the United States must reclaim its role as a leader on global challenges. COVID-19 provides a near-term opportunity where the world will be watching: the United States could play

a leading role coordinating vaccine research, information-sharing, cooperating on industrial mobilization, and providing assistance to impacted nations.[81] Looking beyond the present moment, Washington should signal its recommitment by rejoining the Paris Climate Accords. The U.S. withdrawal allowed China to present itself as the more responsible actor on climate change. Given that 175 parties signed the accords and Washington negotiated specifically with Beijing to ensure both nations joined, the U.S. withdrawal makes it appear the obstreperous party.[82] The list of other global problems is too long to enumerate here,[83] but the basic dynamic for many of them is similar. The United States must reverse this trend by playing a leading role in developing the multilateral responses so that the world sees it as willing to lead and committed to the international order it helped create.

Developing Alternatives to Chinese Statecraft. While the deterrence posture above provides stability, and a return to multilateralism will improve the U.S. image, we must also set the economic conditions to sustain U.S. influence over the long term. Two key elements compose this approach: setting conditions for more reciprocal economic relations and building tools to challenge Chinese economic statecraft.

First, the United States should continue to privately press for fair and reciprocal trade terms in negotiations with China. Today, U.S. firms do not enjoy fair access to Chinese markets, China's state-owned enterprises receive subsidies that make competing difficult for U.S. companies, and China demands access to foreign firms' intellectual property and data before it allows them to do business. The Trump administration has pushed back against these imbalances. Having already pressed these concerns, the United States should continue to pursue them in ongoing negotiations while being clear-eyed about the limits of what China may concede and doing so privately to avoid threatening Beijing's prestige.

This approach, however, has not produced significant results to date—the Phase I trade deal avoided many of these issues. Instead of continuing to press

publicly through aggressive unilateral tariffs—a battleground where China has significant countervailing leverage and will also feel pressure to show toughness—the United States should create multilateral pressure by rejoining the successor agreement to the Trans-Pacific Partnership (TPP). Doing so would require accepting some concessions because negotiations advanced in our absence, but it would be a huge signal to allies skittish about U.S. commitments to regional and multilateral institutions. And ultimately, the combined pressure of TPP members makes it more likely that China will feel compelled to accommodate these demands over time.

This step should, however, be coupled with targeted pressure through the dispassionate application of U.S. law. The United States should, for example, increase the scrutiny placed on Committee on Foreign Investment in the United States cases and broaden its mandate to other business dealings like venture capital investments.[84] The administration should work with Congress to expand sanctions authorities to cut off Chinese firms that illicitly obtain U.S. technology.[85] And the United States should delist Chinese companies that do not meet audit and disclosure requirements for U.S. exchanges.[86] Last, given the significant impacts of cyber-enabled IP theft, the United States should revisit the recommendations of the Commission on the Theft of American Intellectual Property. Those recommendations are sufficiently numerous that a full treatment is not possible here. Suffice it to say that a 2017 update to the commission's report suggested that while the United States has made some progress, many of the commission's recommendations had not been implemented at that time.[87]

Second, the United States should build tools to compete with China's development finance model, in particular BRI. The logic here is also straightforward; it is difficult to "beat something with nothing." The reality is that for all the handwringing in Washington, Chinese financing responds to significant infrastructure gaps (for example, an estimated $26 trillion in Asia through

2030[88]) that traditional finance vehicles were not meeting. U.S. rhetoric warning nations of predatory loans may make China look bad, but it is unlikely to succeed without a credible alternative.

This strategy argues that creating an alternative to BRI is economically viable, especially if the United States does so with other nations and leverages multilateral institutions. The United States has made some progress with its recent Better Utilization of Investments Leading to Development (BUILD) Act, which overhauls the Overseas Private Investment Corporation (OPIC) and provides $60 billion for loans as well as political risk insurance for U.S. commercial entities. Yet $60 billion will not compete favorably with $1 trillion or more in potential Chinese loans.

The United States could address this gap through three steps. First, it should expand the BUILD Act to grow the funds available to the U.S. International Development Finance Corporation (DFC) considerably. Many U.S. commentators have called for an alternative to BRI yet argue that the United States cannot afford to compete symmetrically. It is well within U.S. capacity, however, to grow DFC by several times its current size. This cost appears substantial at first, until one realizes that DFC will be issuing loans, not grants. In fact, DFC's predecessor, OPIC, returned a $3.7 billion profit to the Treasury from 2012 to 2017, and its loans have created 275,000 jobs and $75 billion in U.S. exports since 1974.[89] There would be costs to capitalize the fund, but at the time of this writing, reactions to the coronavirus have left the United States able to borrow at record low rates—so low, in fact, that in inflation-adjusted terms, it is actually being paid to borrow.[90]

Second, the United States should expand the alternatives to BRI by working with key allies, the World Bank, and the Asian Development Bank to expand the types of loans available. Several nations have begun to build similar development finance vehicles and to pursue bilateral or multilateral partnerships to deconflict resources. The United States should demonstrate renewed leadership by

Sailor aboard Royal Canadian Navy ship HMCS *Regina* relays orders to helm on bridge during replenishment-at-sea with Royal Australian Navy ship HMS *Sirius* during RIMPAC, August 20, 2020 (Courtesy Royal Canadian Navy/Dan Bard)

taking this concept further, creating an Infrastructure Development Coalition that creates an integrated structure with other leading nations in development finance.[91]

And last, it should couple these increased development finance offerings with a modest increase in direct development assistance. The U.S. Agency for International Development currently funds assistance to help nations evaluate loan offerings, the technical feasibility of projects, and a variety of supporting programs (for example, legal assistance to strengthen contract enforcement, streamline regulations, and meet labor standards). The agency's fiscal year 2020 budget request included $449 million for the Indo-Pacific region (covering other issues as well). An increase of $3 billion to $5 billion would have substantial impact alongside loan offerings while not radically altering the U.S. debt picture or the percentage of the budget that goes to foreign aid.[92]

Exposing China's Malign Behavior. China is adroit at messaging campaigns that portray it as a peaceful power and its governance model as superior. China's actual behavior, however, tells a different story. To reinforce the objectives above and help nations balance with us, the United States should launch a coordinated information campaign that seeks to expose the differences between China's propagated narratives and its actual conduct. The principal objective should be to expose China's malign practices to foreign audiences to shape their views. At the same time, such messaging might have the collateral benefit of convincing China to corral some behaviors.

The centerpiece of this campaign should be China's treatment of ethnic minorities, in particular the gross mistreatment of Uighurs and other Muslim minorities in Xinjiang Province. The

United States should hold regular press briefings on these activities, declassify U.S. assessments when possible, and amplify nongovernmental leaks that have begun to emerge in Xinjiang.[93] The United States should supplement coverage of this topic with evidence of other human rights abuses and authoritarian behavior, including the detention of regime critics and human rights activists, the expansion of China's surveillance state, and efforts to suppress protests in Hong Kong. The United States should then encourage other nations to amplify this messaging. It should in particular seek to persuade other Muslim nations that have been reluctant to speak out.

This campaign should combine with a second information campaign documenting China's lending practices under BRI, economic coercion of states and corporations, and attempts to export its development model. The United States should showcase BRI's lack of

transparency, cases of poor results, and ways in which BRI acts as a tool for geostrategic leverage, not simply assistance. The messaging should be coordinated to highlight aforementioned efforts to build alternatives to BRI and a multilateral consortium to provide such loans. Here again, Washington should press partners to amplify this message among their publics.

Finally, the United States should launch a media outreach effort focused on Chinese business perfidy. It should highlight China's endemic corruption, use of state-owned enterprises to undercut other nations' competitiveness in global trade, Internet censorship, IP theft, and use of market access to coerce companies to bow to Chinese demands.[94] The United States should look for firms that experienced negative long-term effects and use those firms to amplify this message and display concrete evidence of the impacts Chinese activities have on companies.

Collectively, the elements of this media campaign would reinforce the other objectives above; this effort would not only cast doubt on China's messaging about its responsible behavior but also implicitly juxtapose this behavior to more benign U.S. partnership.

Objective 3: Restore Sources of Long-Term U.S. Domestic Strength. The previous objectives set the initial conditions to sustain U.S. influence in a competition with China. This competition, however, could last decades. Sustaining our efforts over the long term thus requires the United States to be strong domestically, building on many of its aforementioned advantages. The United States has the resources to do so, but these resources must be revitalized to avoid atrophy. The present access to cheap capital and likely future financial injections to provide economic stability provide a propitious window for such action.[95]

The United States should begin by taking steps to ensure the long-term vibrancy of its economy. A full accounting of the steps required is not possible here, but key elements include the following:

- Technology. The United States should seek to maintain its technological edge by increasing R&D funding in key emerging technologies such as artificial intelligence, where it has been less aggressive than China in recent years.[96] Government incentives should be designed to ensure the United States is poised to lead in the technologies and economic sectors most likely to drive future growth (for example, electric vehicle infrastructure, battery technology, solar power, and many others), rather than clinging to legacy manufacturing. It also means promoting a business and regulatory climate designed to support American business and help it to compete against Chinese firms.[97] Moreover, such steps must be coupled with a technology protection regime to defend U.S. innovations from Chinese theft, coercive acquisition, or cooption, while enabling cooperative development with allies and partners.

- Education and human capital. The United States should couple those efforts with investments to ensure that it has the best human capital. This means reinvesting in the U.S. education system, including not only building on our first-rate universities but also investing in universal pre-kindergarten and greater kindergarten through 12th grade science, technology, engineering, and mathematics education. It also requires developing new training models to support working-class citizens as the Nation moves toward artificial intelligence–enabled automation to handle many basic jobs.

- Infrastructure. The United States should revitalize the Nation's infrastructure, not only updating aging infrastructure but also investing in new elements that would unleash American productivity, such as installing high-speed fiber and broadband nationally, which allows people to access virtual high-quality training, to pursue high-paying jobs

that could be done anywhere, and—most critically—to invent.[98]

- Immigration. The United States must expand immigration, which has long been a source of strength and innovation, and reform its approach toward it, including raising the overall cap on visas for advanced degree holders to ensure that the brightest foreign students can stay and contribute their skills to our economy.[99]

- Public health. America's health is a significant comparative advantage to China. But the United States spends more on health care than any nation in the world yet still has the lowest life expectancy among wealthy nations. The rising costs of Medicare and Medicaid are the largest driver of the Federal deficit. And we were no better prepared for the coronavirus than nations that spend much less. There are multiple health care models the United States could pursue with track records in other countries; almost all, however, have two key elements: some form of universal coverage and measures for cost control.[100] Here again, the crisis caused by the pandemic offers an opportunity to adjust the system for the better.

- Energy. The U.S. energy windfall over the past decade transformed a strategic vulnerability into a source of strength. Yet the United States does not behave like an energy superpower. The United States should transform its energy grid (which Thomas Edison would still recognize from the one he designed in the 1890s) to improve its resiliency, develop "swing capacity" by having some state-owned oil wells ready to pump as leverage internationally (most other major energy-producing nations do this; the United States does not), develop regulatory regimes around significant liquid natural gas deals that provide preference for U.S. allies, and launch a national-level initiative through the National Laboratories on renewable energy technology.[101]

Demonstration for rights of Uighurs, Berlin, January 19, 2020 (Courtesy Leonhard Lenz)

These steps are necessarily illustrative, but all would build on advantages the United States has vis-à-vis China, posture the United States to lead in the industries of the future, and sustain domestic vibrancy that will be required in a long-term competition. To support this strategy, the next President should work with Congress to appoint a bipartisan commission with a mandate to bolster U.S. domestic strengths for long-term competition, which should develop a body of proposals, a timeline, and anticipated costs for presentation to Congress or pursued where possible via administration policy.

Additionally, engaging the American people is key to building support for the initiatives outlined here. Given the public's continued desire for services that outstrip tax revenues and common expectations that U.S. actions abroad should impose no hardships on citizens, the administration must initiate a domestic education campaign to frame the challenge China poses and a parallel campaign on our fiscal health. Both campaigns need to help Americans think about these issues in terms of national security, not simply domestic debates about taxation.[102]

Next, just as the initiatives seek to shore up our economic strengths, the administration—working with Congress—should launch a parallel education effort to shore up the integrity of our democratic institutions. Rebuilding confidence in our institutions serves three purposes: to lessen the partisanship that has paralyzed the country, limiting its ability to act decisively; to limit China's ability to portray the U.S. model as dysfunctional and its own model as superior; and to help build buy-in for the commitment of resources needed to sustain a long-term competition with China. A civic education campaign should be the centerpiece of this renewal. Domestic civic knowledge is appallingly bad today.[103] Robust education produces positive effects on voter turnout, school dropout rates, and community activism. This campaign should emphasize the Nation's free press, fair elections, and rule of law—all of which China lacks.[104]

These efforts are essential to sustain a multidecade competition. Given scarce resources, to pursue them also requires U.S. leaders to exercise stark priority-setting, discipline, and risk acceptance. This is more of a mindset than a list of specific activities.

First, the United States should look to reduce tensions with Russia while still defending U.S. alliance commitments. Critically, this is not a "reset"; we should not chase Russian engagement. Nor should we ignore the risk of Russian threats in Eastern Europe or its undermining of U.S. democracy. But since Russia's economic and demographic trends do not suggest a long-term, multidimensional challenge as China's do, we should seek to dial down animosity in this relationship to allow us to focus on the Indo-Pacific region. This should include quiet diplomacy to see where mutual concessions might be possible (while being clear-eyed that none may be) but minimally seeking to lower antagonist rhetoric on both sides. At a minimum, the United States should accept Vladimir Putin's offer for a simple extension of

the New Strategic Arms Reduction Treaty, providing considered stability and removing the potential for a costly competition. Reducing tensions might also decrease incentives for Russia and China's increasing collaboration. And in the long term, it might even play on traditional balancing dynamics. Over time, Russia might come to see China, which it shares a border with and has fought previously, as a bigger threat.[105]

Second, the United States should reduce its military presence in the Middle East and rejoin the Joint Comprehensive Plan of Action.[106] To do so would signal goodwill to European allies but more importantly would lower the risk, at least for a time, of a principal threat driving U.S. force posture in the Middle East today. This is not to suggest the Iran nuclear deal is perfect, but to acknowledge the enormous opportunity costs to any military action there. Simply put, any administration focused on China should do everything possible to diplomatically defuse tensions and avoid conflict with Iran.[107]

Objective 4: Pursue "Principled Engagement" with China. Even as the United States undertakes the steps above, it should be prepared to cooperate with China where doing so serves U.S. interests. Such cooperation might be frustrating and produce little at times, but it is still worth pursuing for several reasons. First, it provides a vehicle for pursuing progress on transnational issues. Second, it signals to China and the rest of the world that even as U.S.-China competition intensifies, the United States is not inherently aggressive or bent on dominance. Third, it provides a venue to establish mechanisms for crisis stability—mechanisms that we had during the U.S.-Soviet era but that are less robust with China today. And last, it provides ballast for the relationship as it becomes more competitive in other areas. Contrary to arguments that a competitive posture is incompatible with such cooperation, it could in fact make competitive policies more effective by giving China a stake in the relationship.[108]

Given the complex nature of the U.S.-China relationship, the agenda for dialogue could take any number of forms. But the motivations above point to some key elements. First, the United States should suggest a dialogue on global issues, starting with climate change. This focus on climate change could be supplemented with dialogue on global health infrastructure, nonproliferation, and humanitarian relief. Second, the defense establishments should build on conversations to date to develop crisis communication channels designed to mitigate tensions and avoid unintended escalation.[109] Third, bilateral engagement should include a dialogue focused on norms on the use of emerging technology such as artificial intelligence, where China and the United States both have interests but rules of the road remain nascent.[110]

Costs and Risks

The costs of this strategy are nontrivial but well within the Nation's means, provided we can marshal political will to do so. The costs of restoring conventional deterrence are in keeping with levels envisioned in the National Defense Strategy. New investment, such as increased R&D or security assistance, could largely be sourced by reprioritization within DOD's planned topline.[111] Many of the actions associated with the second objective involve diplomacy or messaging; these costs are nominal from an overall budget perspective. The two elements with significant costs are the strategy's proposal to create an alternative to BRI and the strategy's objective to renew U.S. domestic strengths. Expanding the U.S. International Development Finance Corporation would also require a significant initial outlay. However, once capitalized, this fund may actually generate revenue, not consume it.

The costs associated with revitalizing U.S. domestic strengths are impossible to estimate with precision but likely would be substantial in the near term. Ideally, such proposals would be offset by action to restore U.S. fiscal solvency—an issue beyond the scope of this article. Absent such proposals, however, the steps above to secure our long-term domestic strengths could still be pursued for some time. The borrowing in response to the coronavirus clearly shows that borrowing funds in the near term is feasible,[112] and the current access to cheap capital presents a unique window.[113] Moreover, these proposals are ones many experts believe are key to long-term competitiveness. This logic suggests these near-term costs might be recouped by long-term gains of a more vibrant economy with technological advantages and premiere human capital in the sectors that matter for growth.

As with any strategy, this approach entails risks. While a full list is impossible to catalog, several are worth considering:

- The American public does not support this approach to China.[114]
- The American public does not support expending the resources to support this strategy
- Other threats emerge that divert U.S. resources.
- Even absent other threats, U.S. leaders lack the discipline to take risk in other regions.
- U.S. actions would cause China to increase aggressive behavior rather than back down.
- U.S. actions would sideline moderate voices within the Chinese regime.
- China might perceive its relative position worsening as the United States begins to focus more resources; it might then choose to act aggressively while it perceives a window of opportunity before the United States is fully poised to focus on it.[115]
- The set of actions here, even if implemented, would be insufficient to succeed, in which case we have angered China but are unable to deny its objectives.

Some considerations might mitigate some of these risks, however. Most significant, the robust political consensus on this issue may guide public sentiment over time. That same consensus also gives some cause for cautious optimism that U.S. leaders would be able to exercise more discipline in other applications of American power. For those risks involving

AAV-P7/A1 assault amphibious vehicles assigned to Combat Assault Company, 3rd Marine Regiment, unload Servicemembers during amphibious landing demonstration as part of RIMPAC, at Pyramid Rock Beach on Marine Corps Base Hawaii, July 29, 2018 (U.S. Marine Corps/Aaron S. Patterson)

unexpected Chinese behavior, one can only say that it is impossible to know with certainty what China might do, but there is an equally plausible case that Beijing's more assertive posture over the past several years is a result of U.S. inaction. The risks of prompting aggressive Chinese reaction are real, but so too are the risks invited by a weak response.[116]

Moreover, the cost of inaction is also unpalatable. While this strategy might entail some costs or hardship, the long-term alternative is a world in which U.S. companies are less competitive and experience more restricted market access, the United States is less able to influence world affairs, individual liberties are increasingly curtailed, and we potentially encounter military aggression we cannot defeat.[117] Examining this alternative future makes clear that the costs of inaction are far greater over the long term. As Secretary of Defense James Mattis stated when

issuing the National Defense Strategy, "America can afford survival."[118]

In *The Sun Also Rises*, one character asked another how someone goes bankrupt: "Gradually, and then suddenly" is the reply. U.S. strategists examining China's rise and U.S. performance over the past few years could be forgiven for fearing the same dynamic. The United States still enjoys a strong position in today's system, yet China's growth presents an ominous challenge. This strategy describes ways to extend enduring U.S. strengths and sustain its position in the international system. To borrow and amend a line attributed to Benjamin Franklin: The United States has advantages, if we can keep them. **JFQ**

- - - - - - - - - - - - - - - - - - - -

Notes

[1] Quoted in Robert D. Blackwill, *Implementing Grand Strategy Toward China: Twen-*

ty-Two U.S. Policy Prescriptions, Council Special Report No. 85 (New York: Council on Foreign Relations, January 2020), available at <https://www.cfr.org/report/implementing-grand-strategy-toward-china>.

[2] Michèle Flournoy, *Department of Defense (DOD) Role in Competing with China*, Testimony Before the House Armed Services Committee, January 15, 2020, available at <https://armedservices.house.gov/_cache/files/4/4/44fbef3d-138c-4a0a-b3a9-2f05c898578f/0E4943A5B-FAEDA465D485A166FABCF5F.20200115-hasc-michele-flournoy-statement-vfinal.pdf>.

[3] For example, see Thomas L. Friedman, "How Trump and Xi Can Make America and China Poor Again," *New York Times*, August 6, 2019, available at <www.nytimes.com/2019/08/06/opinion/trump-china-trade.html>; Elbridge Colby, "How to Win America's Next War," *Foreign Policy*, May 5, 2019, available at <https://foreignpolicy.com/2019/05/05/how-to-win-americas-next-war-china-russia-military-infrastructure/>; Elizabeth C. Economy, "Yes, Virginia, China Is Exporting Its Model," *Council on Foreign Relations*, December 11, 2019, available at <https://www.cfr.org/blog/yes-virginia-chi-

na-exporting-its-model>.

[4] For a detailed treatment of many of these issues, see Michael Beckley, *Unrivaled: Why America Will Remain the World's Sole Superpower* (Ithaca, NY: Cornell University Press, 2018).

[5] See, for example, Graham Allison, "What Xi Jinping Wants," *The Atlantic*, May 31, 2017, available at <www.theatlantic.com/international/archive/2017/05/what-china-wants/528561/>. On China's economic rise and challenges, see Wayne Morrison, *China's Economic Rise: History, Trends, Challenges, and Implications for the United States*, RL33534 (Washington, DC: Congressional Research Service, June 25, 2019).

[6] For example, see Lowy Institute, *Asia Power Index 2019*, available at <https://power.lowyinstitute.org/>. This report concludes that the United States is still the most powerful nation in Asia, but China is quickly catching up. See also Blackwill, *Implementing Grand Strategy Toward China*.

[7] A brief caveat on the coronavirus is required here. What happens in the next few months could have profound implications for the economic foundations of many nations, the future of globalization, and the U.S. position in the world. Yet the pandemic's lasting impacts will not be clear for some time, and there are many structural continuities that will remain features of the international system. This strategy will thus be mindful of, but not dictated by, the current crisis. But it should be reassessed to ensure its continued coherence as this crisis unfolds.

[8] On the value of the international order, see G. John Ikenberry, *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* (Princeton: Princeton University Press, 2011); Michael J. Mazarr and Ashley L. Rhoades, *Testing the Value of the Postwar International Order* (Santa Monica, CA: RAND, 2018), available at <https://www.rand.org/pubs/research_reports/RR2226.html>.

[9] Note that U.S. rhetoric has also shifted to emphasizing the prevention of a rival hegemon. The Trump administration's *Indo-Pacific Strategy Report*, for example, argues for "a vision which recognizes that no one nation can or should dominate the Indo-Pacific." Cited in Ely Ratner et al., *Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific* (Washington, DC: Center for a New American Security [CNAS], December 2019), available at <https://www.cnas.org/publications/reports/rising-to-the-china-challenge>. Robert Blackwill articulates a similar phrase as his preferred political aim. See Blackwill, *Implementing Grand Strategy Toward China*, 9. I have included it as well because I believe the United States should have a *positive* political aim, not just an aim to prevent an outcome. I believe these objectives are compatible and reinforcing.

[10] Morrison, *China's Economic Rise*, 1. Whether China is currently the world's largest or second largest economy depends on how one measures. If measured based on purchasing power parity, China surpassed the United States in 2015. See, for example, International Monetary Fund (IMF), "GDP Based on PPP, Share of World," in *World Economic Outlook: Growth Slowdown, Precarious Recovery* (Washington, DC: IMF, April 2019).

[11] See, for example, Hal Brands and Zach Cooper, "After Responsible Stakeholder, What? Debating America's China Strategy," *Texas National Security Review* 2, no. 2 (February 2019), available at <http://dx.doi.org/10.26153/tsw/1943>.

[12] Allison, "What Xi Jinping Wants"; Katsuji Nakazawa, "Xi's Overly-Ambitious Goals Triggered U.S.-China Trade War," *Nikkei Asian Review*, July 12, 2018, available at <https://asia.nikkei.com/Editor-s-Picks/China-up-close/Xi-s-overly-ambitious-goals-triggered-US-China-trade-war>.

[13] Odd Arne Westad, "The Sources of Chinese Conduct," *Foreign Affairs* (September/October 2019), available at <https://www.foreignaffairs.com/articles/china/2019-08-12/sources-chinese-conduct>; Fei-Ling Wang, "From Tianxia to Westphalia: The Evolving Chinese Conception of Sovereignty and World Order," in *America, China, and the Struggle for World Order: Ideas, Traditions, Historical Legacies, and Global Visions*, ed. G. John Ikenberry, Zhu Feng, and Wang Jisi (New York: Palgrave Macmillan, 2015), 43–62.

[14] Adapted from several sources, the primary being Blackwill, *Implementing Grand Strategy Toward China*.

[15] "Roundtable Discussion on U.S.-China Relations," National War College video-teleconference with Carnegie-Tsinghua Center for Global Policy, April 2, 2019.

[16] Octavian Manea, "The National Defense Strategy a Year Later: A *Small Wars Journal* Discussion with Elbridge Colby," *Small Wars Journal*, January 19, 2019, available at <https://smallwarsjournal.com/jrnl/art/national-defense-strategy-year-later-small-wars-journal-discussion-elbridge-colby>.

[17] Richard Fontaine, "Great-Power Competition Is Washington's Top Priority—but Not the Public's," *Foreign Affairs*, September 9, 2019, available at <www.foreignaffairs.com/articles/china/2019-09-09/great-power-competition-washingtons-top-priority-not-publics>.

[18] "Remarks by Secretary Mattis on National Defense Strategy," Reagan National Defense Forum, Simi Valley, CA, December 1, 2018, available at <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1702965/remarks-by-secretary-mattis-on-national-defense-strategy/>. Mattis argued that "history is clear: Nations with allies thrive. America's alliances are a durable, asymmetric advantage that no competitor in the world can match." Mattis went on to note, for example, that the North Atlantic Treaty Organization represents half of world economic and military might.

[19] The World Economic Forum's Global Competitiveness Index ranks the United States 1st and China 28th. See "How Competitive Is China's Economy on the Global Stage?" *ChinaPower*, April 2, 2018, available at <https://chinapower.csis.org/china-economy-competitiveness/>.

[20] For example, the continued use of the dollar as a global reserve currency.

[21] For example, the United States became the world's largest oil producer in 2018. See U.S. Energy Information Agency, "The United States Is Now the Largest Global Crude Oil Producer," September 12, 2018, available at <https://www.eia.gov/todayinenergy/detail.php?id=37053>.

[22] While some will rightly note that the advent of cyber capabilities decreases the sanctuary the homeland affords, the United States nonetheless remains surrounded by friendly nations or large oceans. China, by contrast, must contend with numerous major powers on its borders.

[23] For details, see Beckley, *Unrivaled*, chapter 3. For example, the United States is home to 50 of the top 100 universities worldwide, compared with China's 2. Three-quarters of Chinese citizens have not completed high school, and roughly one-third of children entering the workforce are barely literate.

[24] For details, see Beckley, *Unrivaled*, chapter 3. For example, by 2050, the number of Chinese over the age of 65 will triple to 33 percent of its population (versus 20 percent for the United States)—a huge economic drag.

[25] Michael J. Mazarr et al., *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives* (Santa Monica, CA: RAND, 2018), 17, available at <https://www.rand.org/pubs/research_reports/RR2726.html>. The authors note that, although the international order is under challenge, it remains the context in which China must execute its challenge—a significant advantage for the United States.

[26] A detailed treatment of these advantages is available in Beckley, *Unrivaled*.

[27] It is worth noting that, although China's economy eclipsing the United States seems inexorable in many narratives, numerous experts made similar projections for Russia and Japan in the 1960s and 1970s. Cited from James N. Miller, "Protecting U.S. Vital Interests in Great Power Competition," unpublished paper prepared for Defense Science Board. Also see David Fickling, "China Could Outrun the U.S. Next Year, or Never," Bloomberg, March 8, 2019, available at <www.bloomberg.com/opinion/articles/2019-03-08/will-china-overtake-u-s-gdp-depends-how-you-count>.

[28] For more on this point, see David Leonhardt, "What Americans Don't Under-

stand About China's Power," *New York Times*, January 16, 2020, available at <www.nytimes.com/2020/01/16/opinion/sunday/china-economy-trade.html>.

[29] Michael Fuchs, "How to Lose Friends and Strain Alliances," *Foreign Affairs*, March 12, 2020, available at <www.foreignaffairs.com/articles/china/2020-03-12/how-lose-friends-and-strain-alliances>.

[30] Joshua Ball, "Secretary Mattis: 'We've Lost the Power of Inspiration; We've Got the Power of Intimidation,'" *Global Security Review*, June 10, 2019, available at <https://globalsecurityreview.com/secretary-mattis-weve-lost-powerinspiration-weve-got-power-intimidation/>.

[31] Melanie Hart and Blaine Johnson, "Mapping China's Global Governance Ambitions," *American Progress*, February 28, 2019, available at <https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/>.

[32] Joseph R. Biden, Jr., "Why America Must Lead Again," *Foreign Affairs* (March/April 2020), available at <www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again>.

[33] Fontaine, "Great-Power Competition Is Washington's Top Priority—but Not the Public's."

[34] The 2017 U.S. National Security Strategy articulates four national interests. However, because "peace through strength" does not appear to be an "interest," it is not treated separately in this article. It is also worth noting that not all scholars or policymakers see values as a vital U.S. interest. I have included it here, however, both because it is a part of the classical formulation of U.S. interests and because China's alternative governance model poses a challenge to U.S. values but could also create a future where these differing values create a less stable world that then presents security and economic challenges as well.

[35] See Elbridge Colby, *The Implications of China Developing a World-Class Military: First and Foremost a Regional Challenge*, Testimony to the U.S.-China Economic and Security Review Commission, June 2019, available at <https://www.cnas.org/publications/congressional-testimony/the-implications-of-china-developing-a-world-class-military-first-and-foremost-a-regional-challenge>. It is for this reason that the National Defense Strategy emphasizes "favorable *regional* balances of power." Emphasis added.

[36] For more on this topic, see Colby, "How to Win America's Next War."

[37] Joe Gould, "China's AI Ambitions Are Driving U.S. Innovation. So What's America's Holdup?" *Defense News*, March 30, 2018, available at <www.defensenews.com/pentagon/2018/03/30/chinas-ai-ambitions-are-driving-us-innovation-so-whats-americas-holdup/>; Martin Giles, "The U.S. and China Are

in a Quantum Arms Race that Will Transform Warfare," *MIT Technology Review*, January 3, 2019, available at <https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/>; David Lague, "China Leads U.S. on Potent Super-Fast Missiles," Reuters, April 25, 2019, available at <www.reuters.com/article/us-china-army-hypersonic/china-leads-u-s-on-potent-super-fast-missiles-idUSKCN1S11E6>.

[38] See David Sanger, *The Perfect Weapon* (New York: Penguin Random House, 2018); Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: DOD, February 2017). See also James N. Miller et al., "The Growing Threat from Cyber Weapons and What the United States Needs to do to Prepare," Brookings Institution, June 6, 2017, available at <https://www.brookings.edu/events/the-growing-threat-from-cyber-weapons-and-what-the-united-states-needs-to-do-to-prepare/>; Michael J. Mazarr et al., *Hostile Social Manipulation: Present Realities and Emerging Trends* (Santa Monica, CA: RAND, 2019), available at <https://www.rand.org/pubs/research_reports/RR2713.html>.

[39] See, for example, "Hacked: How China Stole U.S. Technology for Its J-20 Stealth Fighter," *The National Interest*, July 10, 2019, available at <https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231>.

[40] Steve Johnson, "The Great Haul of China, Illustrated," *Financial Times*, November 19, 2019.

[41] Allison, "What Xi Jinping Wants."

[42] "Factbox: Made in China 2025: Beijing's Big Ambitions from Robots to Chips," Reuters, April 20, 2018, available at <www.reuters.com/article/us-usa-trade-china-policy-factbox/factbox-made-in-china-2025-beijings-big-ambitions-from-robots-to-chips-idUSKBN1HR1DK>.

[43] White House Office of Trade and Manufacturing Policy, "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," June 2018, available at <https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf>.

[44] Erik Sherman, "One in Five U.S. Companies Say China Has Stolen Their Intellectual Property," *Fortune*, March 1, 2019, available at <https://fortune.com/2019/03/01/china-ip-theft/>.

[45] Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," Council on Foreign Relations Backgrounder, May 21, 2019, available at <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>.

[46] Go Yamada, "Is China's Belt and Road Working? A Progress Report from Eight Countries," *Nikkei Asian Review*, March 28, 2018, available at <https://tinyurl.com/y98gap8k>.

[47] Lowy Institute, *Asia Power Index 2019*.

[48] See Timothy S. Rich, "Can the U.S. Help Taiwan Keep Its Remaining Diplomatic Relationships?" *The Diplomat*, May 30, 2019, available at <https://thediplomat.com/2019/05/can-the-us-help-taiwan-keep-its-remaining-diplomatic-relationships/>.

[49] David Sanger and David McCabe, "Huawei Is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives," *New York Times*, February 17, 2020, available at <www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html>.

[50] Jonathan Stromseth, "Don't Make Us Choose: Southeast Asia in the Throes of U.S.-China Rivalry," Brookings Institution, October 2019, available at <www.brookings.edu/research/dont-make-us-choose-southeast-asia-in-the-throes-of-us-china-rivalry/>.

[51] Hendrik Schulte Nordholt, *China and the Barbarians: Resisting the Western World Order* (Leiden: Leiden University Press, 2018), 9.

[52] Louise Lucas, "Inside China's Surveillance State," *Financial Times*, September 8, 2018, available at <www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543>; Nicole Kobie, "The Complicated Truth About China's Social Credit System," *Wired*, June 7, 2019, available at <www.wired.co.uk/article/china-social-credit-system-explained>.

[53] Austin Ramsey and Chris Buckley, "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims," *New York Times*, November 16, 2019, available at <www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html>; Rob Schmitz, "Ex-Detainee Describes Torture in China's Xinjiang Re-Education Camp," National Public Radio, November 13, 2018, available at <https://www.npr.org/2018/11/13/666287509/ex-detainee-describes-torture-in-chinas-xinjiang-re-education-camp>; Vicky Xiuzhong Xi et al., *Uyghurs for Sale: "Re-Education," Forced Labour, and Surveillance Beyond Xinjian*, Policy Brief Report No. 26/2020 (Canberra: Australian Strategic Policy Institute, March 1, 2020), available at <https://www.aspi.org.au/report/uyghurs-sale>.

[54] George Gao, "Why Is China So . . . Uncool?" *Foreign Policy*, March 8, 2017, available at <https://foreignpolicy.com/2017/03/08/why-is-china-so-uncool-soft-power-beijing-censorship-generation-gap/>.

[55] Economy, "Yes, Virginia, China Is Exporting Its Model"; Westad, "The Sources of Chinese Conduct."

[56] Robert Kagan, *Democracy and Disorder: The Strongmen Strike Back* (Washington, DC: Brookings Institute, March 14, 2019), available at <https://www.brookings.edu/research/the-strongmen-strike-back/>.

[57] Ely Ratner, "There Is No Grand Bargain with China," *Foreign Affairs*, November 27, 2018, available at <www.foreignaffairs.com/

articles/china/2018-11-27/there-no-grand-bargain-china>.

[58] Stephen Walt provides a classical formulation that "states will join alliances in order to avoid domination by strong powers." Stephen M. Walt, "Alliance Formation and the Balance of World Power," *International Security* 9, no. 4 (1985), 5. Of note, while other states might balance collectively, India deserves special consideration in this regard. While India's economic and military power is far behind China's today, demographics—a factor often proffered to demonstrate China's inexorable heft—skew heavily in India's favor over time. China is currently aging rapidly while India is home to the largest youth population of any country in history. The United Nations predicts India will surpass China's population by 2027; by 2050, India will stand at 1.5 billion, compared with China's 1.1 billion. How India will rise, and how it will balance given its historic nonaligned status, remains to be seen. But its rise alone might produce the counterweight to complicate the Chinese calculus over time, enabling this theory of victory.

[59] For example, see Minxin Pei, "China's Coming Upheaval," *Foreign Affairs* (May/June 2020), available at <www.foreignaffairs.com/articles/united-states/2020-04-03/chinas-coming-upheaval>.

[60] Beckley, *Unrivaled*; Ruchir Sharma, "The Comeback Nation," *Foreign Affairs* (May/June 2020), available at <www.foreignaffairs.com/articles/united-states/2020-03-31/comeback-nation>.

[61] Michael Mazarr conducted an extensive study of the order in 2015 and found it to be surprisingly resilient, which supports this finding; Mazarr's study, however, predated the Trump administration, whose rhetoric has been hostile to key elements of the order. See Michael J. Mazarr, *Summary of the Building a Sustainable International Order Project* (Santa Monica, CA: RAND, 2018), available at <https://www.rand.org/pubs/research_reports/RR2397.html>.

[62] See, for example, Jeff M. Smith. "China's Rise and (Under) Balancing in the Indo-Pacific: Putting Realist Theory to the Test," *War on the Rocks*, January 8, 2019, available at <https://warontherocks.com/2019/01/chinas-rise-and-under-balancing-in-the-indo-pacific-putting-realist-theory-to-the-test/>.

[63] See Richard B. Andres, "National Security and U.S. Constitutional Rights: The Road to Snowden," in *Cybersecurity and Human Rights in the Age of Cybersurveillance*, ed. Joanna Kulesza and Roy Balleste (Lanham, MD: Rowman & Littlefield, 2015). Andres at one point argues that China's leaders may not be able to make concessions because they believe those concessions would fundamentally undermine regime stability.

[64] For a useful primer on this question, see Steven Van Evera, "The 'Spiral Model' v. the 'Deterrence Model,'" unpublished handout, September 10, 1997, available at <http://web.mit.edu/17.423/www/Archive98/handouts/spiral.html>.

[65] Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies* 33, no. 4 (August 2010), 492, calls this a "moment of maximum danger."

[66] The steps listed here are necessarily illustrative, but are consistent with themes from the National Defense Strategy. For more detail on these force requirements, see Christopher M. Dougherty, *Why America Needs a New Way of War* (Washington, DC: CNAS, June 2019), available at <https://www.cnas.org/publications/reports/anawow>.

[67] Elbridge A. Colby, *Hearing on Implementation of the National Defense Strategy*, Testimony Before the Senate Armed Services Committee, January 29, 2019, available at <https://www.armed-services.senate.gov/imo/media/doc/Colby_01-29-19.pdf>; Eric Heginbotham and Jacob L. Heim, "Deterring Without Dominance: Discouraging Chinese Adventurism Under Austerity," *The Washington Quarterly* 38, no. 1 (Spring 2015), 185–199.

[68] Dougherty, *Why America Needs a New Way of War*.

[69] See Defense Science Board, *Task Force on Cyber Deterrence*. See also O'Hanlon, "Cyber Threats and How the U.S. Should Prepare." The Defense Science Board argues that to address such issues, DOD should undertake efforts at cyber-hardening a portion of its nuclear command and control, long-range conventional strike, and offensive cyber capabilities.

[70] See Hal Brands, Eric S. Edelman, and Thomas G. Mahnken, *Credibility Matters: Strengthening American Deterrence in an Age of Geopolitical Turmoil* (Washington, DC: Center for Strategic and Budgetary Assessments, 2018), available at <https://csbaonline.org/uploads/documents/Credibility_Paper_FINAL_format.pdf>.

[71] DOD has grown its budget by $42 billion over the past 5 years and is proposing another 10 percent in the fiscal year 2020 budget request. This increase was a priority for former Acting Secretary of Defense Patrick Shanahan in particular.

[72] Correspondence with Jim Mitre, vice president for analysis at Govini.

[73] For more on this issue, see Flournoy, Testimony Before the House Armed Services Committee. It is worth noting that the National Defense Strategy has a theory of technological advancement that argues commercial technology adaptation and integration are in some respects more critical than actual R&D, yet DOD lacks both the personnel and the risk-taking incentives to conduct more aggressive experimentation and prototyping.

[74] Henry Farrell and Abraham Newman, "The Twilight of America's Financial Empire," *Foreign Affairs*, January 24, 2020, available at <www.foreignaffairs.com/articles/2020-01-24/twilight-americas-financial-empire>.

[75] Presentation by Dr. Zachary Abuza, professor of National Security Strategy at the National War College.

[76] Luiza Savage, "The U.S. Left a Hole in Leadership on Climate. China Is Filling It," *Politico*, August 15, 2019, available at <www.politico.com/story/2019/08/15/climate-china-global-translations-1662345>.

[77] Bonnie Glaser, "China's Evolving Role in the United Nations: A Conversation with Courtney Fung," *ChinaPower* podcast, June 18, 2019, available at <https://chinapower.csis.org/podcasts/chinas-evolving-role-in-the-united-nations/>.

[78] See, for example, Dan Pearson, "Fix the WTO Appellate Body While We Can," *The Hill*, February 13, 2020, available at <https://thehill.com/blogs/congress-blog/politics/482948-fix-the-wto-appellate-body-while-we-can>.

[79] Some commentators called this "the beginning of the end of the WTO as we know it." "WTO Judge Blockage Could Prove 'the Beginning of the End,'" Deutsche Welle, October 12, 2019, available at <www.dw.com/en/wto-judge-blockage-could-prove-the-beginning-of-the-end/a-51613082>; Tom Miles, "U.S. Blocks WTO Judge Reappointment as Dispute Settlement Crisis Looms," Reuters, August 27, 2018, available at <www.reuters.com/article/us-usa-trade-wto/u-s-blocks-wto-judge-reappointment-as-dispute-settlement-crisis-looms-idUSKCN1LC19O>.

[80] "Brussels Builds Alliance to Bypass U.S. Block on WTO Judges," *Financial Times*, January 24, 2020, available at <www.ft.com/content/e644ffea-3e97-11ea-b232-000f4477f-bca>.

[81] Kurt M. Campbell and Russ Doshi, "The Coronavirus Could Reshape Global Order," *Foreign Affairs*, March 18, 2020, available at <www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order>.

[82] The United States should of course support efforts to meet its own climate change goals if China does so. However, it is also worth noting in this context that since commitments under the Paris Accords are voluntary—and many nations have not met their goals—it is hard to imagine a context in which the United States bore fewer costs for staying in the agreement and bore higher reputational costs for leaving it.

[83] To give one example, migration may not be a direct element of U.S.-China competition, but it is another place where the United States could reassume historic leadership that it has relinquished, which would have significant benefits for America's image abroad as well as long-term economic benefits for the Nation. See Ariana A. Berengaut and Antony J. Blinken, "Trump's Huge Mistake on Refugees," *New York Times*, September 11, 2018, available at

<www.nytimes.com/2018/09/11/opinion/syria-trump-refugees-quotas-discrimination.html>.

84 Ratner et al., *Rising to the China Challenge*; Blackwill, *Implementing Grand Strategy Toward China*.

85 Ratner et al., *Rising to the China Challenge*.

86 Ibid.

87 Dennis C. Blair and Jon M. Huntsman, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and the United States Policy* (Seattle: The National Bureau of Asian Research, 2017), 1–19.

88 Michael Peel and Tom Mitchell, "Asia's $26tn Infrastructure Gap Threatens Growth, ADB Warns," *Financial Times*, February 27, 2017, available at <www.ft.com/content/79d9e36e-fd0b-11e6-8d8e-a5e-3738f9ae4>.

89 Daniel Runde, "We Shouldn't Be Eliminating OPIC, We Should Be Putting It on Steroids," Forbes, April 5, 2017, available at <www.forbes.com/sites/daniel-runde/2017/04/05/we-shouldnt-be-eliminating-opic-we-should-be-putting-it-on-steroids/#6204e3343156>.

90 Jordan Weissman, "The Federal Government Can Borrow Money for Less than Ever. Maybe We Should Take Advantage of That," *Slate*, March 11, 2020, available at <https://slate.com/business/2020/03/government-borrow-bond-yield-infrastructure-coronavirus.html>.

91 William C. Pacatte, *Competing to Win: A Coalition Approach to Countering BRI* (Washington, DC: Center for Strategic and International Studies, December 2019), available at <https://www.csis.org/analysis/competing-win-coalition-approach-countering-bri>.

92 I learned of this consideration from Patrick Ventrell, director of the Bureau of International Narcotics and Law Enforcement Affairs' Office for Western Hemisphere Programs, who also suggested the provision of direct foreign aid, though he recommended a slightly higher amount. A more detailed estimate of the proper funding requirement would require U.S. Agency for International Development expertise.

93 Steve Inskeep, interview with Adrian Zenz, "Leaked Documents Offer a Peek Inside China's Detention of Uighurs," National Public Radio, November 25, 2019, available at <https://www.npr.org/2019/11/25/782549071/leaked-documents-offer-a-peek-inside-chinas-detention-of-uighurs>.

94 The list of companies that have genuflected in the face of Chinese pressure is long. Some of the best-known examples include Marriott, Google, the airline industry, and the National Basketball Association. See, for example, "Marriott's Pitiful Apology to China," *Washington Post*, January 24, 2018, available at <www.washingtonpost.com/opinions/marriotts-pitiful-apology-to-china/2018/01/24/92353716-0083-11e8-86b9-8908743c79dd_story.html>;_ Jamie Davies, "So Much for 'Don't Be Evil' as Google Bows to China Censorship—Sources," *Telecoms*, August 2, 2018, available at <https://telecoms.com/491253/so-much-for-dont-be-evil-as-google-bows-to-china-censorship-sources/>; "Major U.S. Airlines Bow to China's 'Orwellian' Demands on Taiwan Recognition," CBS News, July 25, 2018, available at <www.cbsnews.com/news/airlines-china-taiwan-country-demand-white-house-called-orwellian-nonsense/>; Bari Weiss, "The World's Wokest Sports League Bows to China," *New York Times*, October 8, 2019, available at <www.nytimes.com/2019/10/07/opinion/nba-china-hong-kong.html>.

95 Several of the following ideas draw on work from a *New York Times* multi-essay project called "The America We Need." The introductory essay, titled "A Nation Tested," is available at <www.nytimes.com/interactive/2020/opinion/america-inequality-coronavirus.html?action=click&pgtype=Article&state=default&module=styln-opinion-inequality-series&variant=show&region=TOP_BANNER&context=opinion-inequality-menu>.

96 There are many other specifics that could sit within this recommendation. For more, see Ratner et al., *Rising to the China Challenge*. As one example, this report's examination of this subject recommended "increased access to government data for artificial intelligence and machine learning and efforts to secure semiconductor supply chains." Length restrictions preclude recommendations of that detail here.

97 As one example, Dougherty, *Why America Needs a New Way of War*, argues for regulatory frameworks to accelerate financial technology in competition with foreign jurisdictions and to encourage research into blockchain technology.

98 See Thomas L. Friedman, "Post-Pandemic, Here's How America Rises Again," *New York Times*, April 14, 2020, available at <www.nytimes.com/2020/04/14/opinion/stimulus-infrastructure-covid.html>.

99 For more on this topic, see Vikram J. Singh, "The Great American Brain Drain Is Coming," CBS News, May 23, 2019, available at <www.cbsnews.com/news/commentary-the-great-american-brain-drain-is-coming/>. Additional information is available in Ratner et al., *Rising to the China Challenge*.

100 Anne Case and Angus Deaton, "America Can Afford a World-Class Health System. Why Don't We Have One?" *New York Times*, April 14, 2020, available at <www.nytimes.com/2020/04/14/opinion/covid-inequality-health-care.html>.

101 Several ideas here come from email exchanges with a professor at the National War College who specializes in these issues.

102 For example, former Chairman of the Joint Chiefs of Staff Admiral Michael Mullen cited the national debt as the greatest national security threat. See Tyrone C. Marshall, Jr., "Debt Is Biggest Threat to National Security, Chairman Says," *DOD News*, September 22, 2011, available at <https://archive.defense.gov/news/newsarticle.aspx?id=65432>.

103 Blackwill, *Implementing Grand Strategy Toward China*, 18.

104 Only 26 percent of Americans can name the three branches of government. This point, and the broader recommendation, are taken from Blackwill, *Implementing Grand Strategy Toward China*, 18.

105 Westad, "The Sources of Chinese Conduct." Also Blackwill, *Implementing Grand Strategy Toward China*, 36 (though I would not support all of the specific prescriptions he offers).

106 This has been a goal of U.S. defense strategy since at least 2012 and has rarely been achieved. One former DOD official privately likened the way DOD continued to send the majority of its forces to the Middle East as like "having a $5 million insurance premium on a $500,000 house."

107 Blackwill, *Implementing Grand Strategy Toward China*, 23.

108 Jeffrey A. Bader, *U.S.-China Relations: Is It Time to End the Engagement?* Policy Brief (Washington, DC: Brookings Institution, September 2018), available at <https://www.brookings.edu/research/u-s-china-relations-is-it-time-to-end-the-engagement/>. Flournoy makes a similar point in her testimony before the House Armed Services Committee.

109 Flournoy, Testimony Before the House Armed Services Committee.

110 Ratner et al., *Rising to the China Challenge*.

111 While some commentators have called for a $1 trillion defense budget, other experts argue that this approach could be done with little to no increases. For example, see Kathleen Hicks, "Getting to Less," *Foreign Affairs* (March/April 2020), available at <www.foreignaffairs.com/articles/2020-02-10/getting-less>.

112 William D. Lastrapes, "The U.S. Owes $23.5 Trillion—but Can Still Afford a Big Coronavirus Stimulus Package," *The Conversation*, March 18, 2020, available at <https://tinyurl.com/yb7t49x4>.

113 See Friedman, "Post-Pandemic, Here's How America Rises Again."

114 Fontaine, "Great-Power Competition Is Washington's Top Priority—but Not the Public's."

115 Flournoy, Testimony Before the House Armed Services Committee.

116 See Blackwill, *Implementing Grand Strategy Toward China*, 8.

117 Adapted from Ratner, "There Is No Grand Bargain with China."

118 "Remarks by Secretary Mattis on National Defense Strategy."

Pardon the Paradox
Making Sense of President Trump's Interventions in Military Justice

By Jeremy McKissack

Lieutenant Colonel Jeremy McKissack, USAFR, wrote this paper while attending the Air War College. It won the Strategy Paper category of the 2020 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

Army captain and attorney Aubrey Daniel III wrote a blistering letter to President Richard Nixon in April 1971.[1] The lead prosecutor in the court-martial of First Lieutenant William Calley, Captain Daniel had convinced a military jury at Fort Benning, Georgia, to convict Lieutenant Calley for the murder of at least 22 Vietnamese civilians in the village of My Lai on March 16, 1968.[2] A day after Calley began serving his sentence of life imprisonment, President Nixon reacted to the public outcry against the verdict and ordered the Army to release Calley and return him to his apartment on post.[3] In his letter, Daniel wrote that the President's intervention had "damaged the military judicial system and lessened any respect it may have gained as a result of the proceedings."[4]

Nearly 50 years later, echoes of Captain Daniel's criticism of President Nixon could be heard when another President, Donald J. Trump, intervened in military justice proceedings. In just his first term, President Trump has intervened several times in war crime cases brought under the Uniform Code of Military Justice (UCMJ).[5] He has used

Rear Admiral Collin Green, commander, Naval Special Warfare Command (right), and Force Master Chief William King speak to junior officers and senior enlisted leaders during troop leadership class at Center for SEAL and SWCC, Coronado, California, February 13, 2020 (U.S. Navy/David Schwartz)

his pardon power to terminate one military prosecution, ordered the release of an accused Servicemember from pretrial confinement, and directed the outcome of a military administrative board, all against the recommendations of his senior military advisors.[6] In total, President Trump has granted executive clemency, or pardons, to four Servicemembers accused or convicted of committing war crimes while deployed to Iraq or Afghanistan.[7] His decisions in these cases have elicited widespread criticism from academics, journalists, and retired military leaders.[8]

The criticism of President Trump's war crime pardons has been partially right and partially overstated. The purpose of this essay is to analyze two broad critiques that have emerged from the military pardon cases. It begins with a brief factual and legal overview of the four cases. Next, the essay tackles the first main

argument against the military pardons, which is that President Trump meddled in the military justice process and thereby eroded trust between himself and military leaders. The essay then addresses normative arguments against the pardons that claim they will diminish the military's moral standing and authority and open the floodgates for Servicemembers to commit war crimes with impunity. In the end, the essay attempts to make sense of President Trump's decisions, through the Jacksonian tradition in American politics and foreign policy.

The essay concludes with two recommendations. First, in response to the military pardons, the Department of Defense (DOD) should review its law of war policies, address any deficiencies in them, and implement regular training that highlights the "fundamental importance" of the law of war to the Armed Forces of the United States.[9] Second,

Congress should review the cases to ensure that military law and policy clearly demarcate the role of the commander in chief in the military justice process and that Servicemembers who report war crimes receive full protection from retaliation.

The Military Pardon Cases: A Factual and Legal Overview

The military pardon cases involved four Servicemembers, three from the Army and one from the Navy: Army First Lieutenant Michael Behenna, Army First Lieutenant Clint Lorance, Army Major Mathew Golsteyn, and Navy Chief Petty Officer and SEAL Edward Gallagher. Lieutenant Behenna received his pardon for murder in a war zone in May 2019.[10] Several months later and on the same day, President Trump granted executive clemency to Lieutenant Lorance, Major Golsteyn,

and Chief Petty Officer Gallagher for war crimes.[11] All four cases share similarities. First, the four Servicemembers were either convicted or accused of murdering civilians who were out of combat. Second, the cases reportedly made their way to the President's desk through right-wing media coverage and direct lobbying from individuals or organizations outside government.[12] And third, support for the military pardons split along partisan lines, with one poll revealing that 79 percent of Republicans and only 12 percent of Democrats agreed with Trump's pardon of Lieutenant Lorance.[13]

The four cases are also factually and legally distinct. The parameters of this essay do not allow for a complete treatment of the cases. What follows instead is a summary of the important and distinguishing factual and legal circumstances in each case.

First Lieutenant Michael Behenna. Lieutenant Behenna's actions that led to his conviction for unpremeditated murder occurred not within the fog of war but inside the haze of a fast-moving, dynamic situation largely of his own creation while he was deployed to Iraq in 2008. After being directed to return Iraqi detainee Ali Mansur to his village, Behenna instead ordered his platoon to drive Mansur to a remote section of the Iraqi desert near the area of Albu-Toma.[14] Behenna ordered Mansur to strip naked and sit inside a culvert.[15] Behenna then aimed his firearm at Mansur and attempted to interrogate him.[16] When Behenna averted his attention momentarily, he claimed that Mansur lunged for the firearm, forcing him to shoot Mansur in the head and chest in self-defense.[17]

At trial, the jury rejected Behenna's self-defense argument, and he was convicted and sentenced to confinement.[18] On appeal, the Court of Appeals for the Armed Forces, the military's highest appellate court, ruled against Behenna in a three-to-two decision, holding that Behenna had forfeited the right to self-defense because of his actions vis-à-vis Mansur.[19] One commentator observed that the court's narrow ruling meant that the legal debate about Behenna's right

to self-defense was anything but "open and shut."[20] Furthermore, 37 generals and admirals, along with a former DOD inspector general, had signed a legal brief supporting Behenna's self-defense argument.[21]

In announcing Behenna's pardon, the White House press release did not mention the facts of the case.[22] Instead, the announcement highlighted the unsettled debate about Behenna's self-defense argument.[23] The White House also noted that Behenna had the support of some elected officials and had been a model prisoner.[24]

First Lieutenant Clint Lorance. During his deployment to Afghanistan in 2012, Lieutenant Lorance ordered his troops to fire on three Afghan civilians. At Lorance's court-martial, a platoon member testified to being the first to see three Afghan men riding on a motorcycle enter in "his field of view."[25] The platoon member did not perceive a "definitive hostile intent and hostile act" from the three men. Still, Lorance ordered him to fire without asking whether the three men had shown hostile actions, but the shots missed. Aware of the shots, the men got off the motorcycle. "As they returned to the motorcycle, [Lorance], over his portable radio, ordered the platoon's gun truck to engage the men," killing two of them and injuring a third. Afterward, Lorance's actions seemed designed to cover up and disguise the circumstances surrounding the shooting.

A jury convicted Lorance of murder and attempted murder, among other things, and sentenced him to confinement for 20 years. After Lorance's trial, the government discovered information about the motorcycle passengers that perhaps could have been helpful to Lorance's defense. One of the victims "knew someone who was linked to hostile action against U.S. forces." The other slain passenger "was biometrically linked to an [improvised explosive device] incident" that had occurred prior to the shooting. Finally, the government somehow learned that sometime after the shooting, the wounded passenger took hostile action against U.S. forces. Lieutenant Lorance knew none of this at

the time he ordered his Soldiers to fire. The Army appellate court reviewed the facts and legal arguments and upheld Lorance's conviction and sentence.

Major Mathew Golsteyn. Major Golsteyn traveled a circuitous path to his pardon from President Trump. While deployed to Afghanistan in 2010, Golsteyn, by his own admission, shot an Afghan civilian and buried him in a shallow grave.[26] Golsteyn suspected the civilian of being a Taliban bombmaker.[27] The next day, Golsteyn and two other Soldiers exhumed the body, brought the remains back to base, and burned them.[28] Golsteyn stated that he took matters into his own hands because there was not enough evidence to detain the suspected bombmaker for more than 24 hours.[29] Golsteyn told investigators that he would not have been able to live with himself had the civilian killed more Servicemembers after being released from U.S. custody.[30]

Golsteyn's actions came to light during a preemployment polygraph for the Central Intelligence Agency.[31] The Army launched a criminal investigation in 2011 but decided not to prosecute Golsteyn for lack of evidence.[32] Then, in October 2016, Fox News ran a feature about rules of engagement and interviewed Golsteyn for the program.[33] Golsteyn admitted to the interviewer that he had killed the civilian.[34] Two months later, the Army began investigating Golsteyn once again.[35] The investigation ended with Golsteyn being charged with murder, and he was nearing the start of his court-martial when President Trump intervened and pardoned him.[36]

Chief Petty Officer Edward Gallagher. A Navy SEAL and decorated combat veteran, Edward Gallagher was accused of murdering a wounded captive who belonged to the so-called Islamic State (IS) while deployed to Iraq in 2017.[37] After a firefight, Gallagher learned that an IS fighter had been captured, and he directed his unit to drive to the scene where the captive lay injured and barely conscious.[38] After the SEALs arrived, someone got video footage of Gallagher kneeling next to the detainee and starting medical treatment. A hand is then seen

covering the camera. While appearing to treat the wounded fighter, Gallagher allegedly stabbed him in the neck with a hunting knife. Afterward, Gallagher and other SEALs took a photograph with the IS fighter's corpse. Gallagher's actions came to light when members of the SEAL team, after returning to the United States, reported them to the chain of command and Navy criminal investigators.[39] At the end of the investigation, the Navy charged Gallagher for murdering the IS captive and posing with the corpse.[40]

After Gallagher was charged, evidence came to light that he may have been intimidating or threatening witnesses.[41] Consequently, Gallagher was ordered into pretrial confinement in September 2018.[42] Gallagher's family and legal defense team went public with the case on Fox News, which helped them garner support from some elected officials and President Trump.[43] On March 30, 2019, the President intervened and ordered Gallagher released from jail and into less restrictive confinement on the military installation.[44]

The government's prosecution of Gallagher gradually derailed. First, the judge removed the lead military prosecutor from the case because of "accusations of prosecutorial misconduct."[45] Second, a key witness changed his story on the witness stand, testifying that he, not Gallagher, killed the IS captive.[46] The jury acquitted Gallagher of murder but convicted him of taking a picture with the body. Gallagher was sentenced to a reduction in rank from E7 (chief petty officer) to E6 (petty officer 1st class) and four months' confinement.[47]

When President Trump pardoned Lorance and Golsteyn, he also directed that the Navy restore Gallagher's rank to chief petty officer—reversing the sentence of the trial court.[48] The President, however, did not pardon Gallagher, meaning Gallagher's conviction for posing with the captive's corpse remains undisturbed.[49] Meanwhile, the SEAL command moved full steam ahead to hold an administrative hearing, called a Trident Review Board, to determine whether Gallagher, who intended to retire from the military, would

remain a SEAL and retain the privilege of wearing the gold Trident pin on his uniform.[50] President Trump, nonetheless, swooped in once more to aid Gallagher. On November 21, 2019, the President took to Twitter to announce, "The Navy will NOT be taking away Warfighter and Navy Seal Eddie Gallagher's Trident Pin. This case was handled very badly from the beginning. Get back to business!"[51]

Then–Secretary of the Navy Richard Spencer was not enthusiastic about President Trump's interference in an administrative process involving the SEALs.[52] Spencer wanted the board to go forward.[53] He attempted to salvage the process by brokering a deal with the White House without first coordinating his proposal with Secretary of Defense Mark Esper.[54] On learning of Spencer's behind-the-scenes negotiations, Secretary Esper requested Spencer's resignation, which Spencer promptly tendered.[55] As for Gallagher, he retired from the Navy with his full rank and his SEAL Trident.[56]

Critiquing the Criticism of the Military Pardons Cases

One overarching criticism of President Trump's pardons of Behenna, Lorance, Golsteyn, and Gallagher is that he meddled in predominantly military matters over the recommendations of his civilian and uniformed advisors.[57] In civil-military relations, the phrase *civilian meddling* denotes unwarranted or unnecessary civilian interference or intrusion in military affairs.[58] By interfering or intruding in military affairs, civilians risk undermining military professionalism, which chips away at the Huntingtonian model of "objective control"—a theory of civil-military relations that the military tends to favor.[59]

The notion of civilian meddling entered the civil-military lexicon by way of Samuel Huntington's book *The Soldier and the State*. Published in the 1950s, *The Soldier and the State* posited that true civilian control of the American military occurred through "professionalizing the military."[60] According to Huntington, civilian control increases with "the recognition of autonomous military professionalism."[61] Autonomy

achieved through professionalization not only minimizes military power but also produces a political neutrality or sterility among military officers.[62] Because military officers have been entrusted with overseeing military affairs with little to no oversight from their civilian leaders, their independence to perform their duties as professionals reduces their political power and increases civilian control of the Armed Forces.[63]

Professor Eliot Cohen calls Huntington's objective control the "normal theory" of civil-military relations.[64] For his part, Cohen offered a competing theory to objective control that he labeled "unequal dialogue." In an unequal dialogue, civilian and military leaders engage in frank exchanges and discussions, yet the final authority always rests with the President.[65] Where Cohen pushes beyond the normal theory is in his argument that civilian leaders also have the authority, even the responsibility, to immerse themselves in military affairs and to constantly interact with and ask questions of military leaders.[66]

The Huntington-Cohen frames are by no means the alpha and omega of the civil-military relations literature on civilian control. But these two influential theories serve as purposeful bookends for evaluating whether President Trump's pardons evidenced civilian meddling.

The military pardons cases often get lumped together and painted with a broad brush. A more evenhanded assessment of President Trump's decisions requires an understanding of each case's procedural posture at the time of the pardons. The distinctions matter to the overall conclusion that President Trump's interventions demonstrate obvious civilian meddling in the Golsteyn and Gallagher cases but no meddling at all in those of Behenna and Lorance.

To begin with, few constitutional powers are as absolute as the power of the President to issue pardons and grant executive clemency. Article II, Section 2, of the U.S. Constitution gives the President the "Power to Grant Reprieves and Pardons for Offences against the United States, except in Cases of Impeachment."[67] Presidential authority

Former Secretary of the Navy Richard Spencer delivers remarks during joint regional discussion on sexual assault and sexual harassment at State University of New York, in New York City, September 5, 2019 (U.S. Navy/Sarah Villegas)

to grant executive clemency extends to Servicemembers punished under the UCMJ.[68] With this in mind, we first consider the Behenna and Lorance pardons.

Behenna and Lorance had been tried, convicted, and sentenced before President Trump pardoned them.[69] Their cases had received appellate review. President Trump did not intervene in the cases or direct military authorities to take any particular action with respect to them. The cases, therefore, were ripe for pardon consideration. When viewed as acts of Presidential mercy, the Behenna and Lorance pardons do not evidence civilian meddling. This, of course, does not mean that President Trump *should have* pardoned Behenna and Lorance; that is a separate criticism. Nevertheless, these pardons evidence much less meddling than do the Golsteyn and Gallagher cases. And it is difficult to see why or how the Behenna or Lorance pardons would affect civil-military relations. The

fact that President Trump may have pardoned Behenna and Lorance against the recommendations of his military advisors should not be too alarming, especially when viewed in light of Cohen's unequal dialogue.

In contrast, President Trump's interventions in the Golsteyn and Gallagher cases are good examples of civilian meddling. As for Golsteyn, he was pending trial when the President pardoned him. Granted, the President can pardon anyone charged or convicted of a Federal offense at any stage of a criminal proceeding.[70] Yet Presidents generally wait until trials have concluded, appeals have been exhausted, and sentences have been served before granting pardons.[71] Months before President Trump pardoned Golsteyn, he told reporters that "it was very possible" that he would allow the trials to proceed and make his decision afterward.[72] As it turned out for Golsteyn, nevertheless, he never had to face an

actual trial, unlike Lorance, Behenna, and Gallagher.

The Golsteyn outcome is a bit of a mixed bag when it comes to civilian meddling. An argument in favor of President Trump's intervention prior to trial rests on his authority as commander in chief. Under the UCMJ, for example, the President can convene or send charges to a court-martial, just like a military commander.[73] By the same token, the President probably could order charges withdrawn and dismissed from a court-martial.

But President Trump did not exercise court-martial convening authority–like powers in Golsteyn's case. He used the power of the pardon to put an end to the Army's prosecution before prosecutors even had the opportunity to present evidence to a jury. By doing so, the President tipped the scales of justice in favor of the accused and denied the government the chance to present its case

in a public trial. With his pretrial pardon, President Trump further signaled that he did not trust the Army to reach a fair and just result "after nearly a decade-long inquiry and multiple investigations."[74]

A fair criticism, then, is that President Trump meddled unnecessarily in the Golsteyn case. Although the President's intervention in the case was highly unusual, proponents could counter that he had to get involved given the Army's handling of the case. Conversely, the Army's delays in bringing Golsteyn to court-martial may have been the result of other factors, such as the availability of witnesses and the discovery of additional evidence. Even though President Trump asserted civilian control when he overrode his military advisors and pardoned Golsteyn, he should have allowed the trial to move forward. As it stands, Golsteyn, by his own admission, shot an unarmed Afghan, hid the remains, and emerged relatively unscathed.[75]

The multiple interventions in the Gallagher case, however, more clearly opened the President to charges of civilian meddling. First, President Trump, reacting to Fox News reporting and lobbying from some public officials, ordered Gallagher moved into less restrictive confinement.[76] When he was Secretary of the Navy, Richard Spencer claimed that the President twice asked him "to lift Gallagher's confinement in a Navy brig," which Spencer resisted before ultimately being ordered to move Gallagher to the equivalent of enlisted barracks to await trial.[77] Journalist David Ignatius reported that President Trump even proposed a pretrial pardon for Gallagher, but Spencer talked him out of it.[78]

As commander in chief, President Trump probably had the UCMJ authority to change the conditions of Gallagher's pretrial confinement.[79] But not since President Nixon's intervention in the Calley court-martial had a commander in chief inserted himself in a court-martial proceeding to the extent that President Trump did in Gallagher's case.[80] After resigning as Secretary of the Navy, Spencer wrote that "military justice works best when senior leadership stays far away."[81] Here, the President,

at the behest of political allies, put his thumb on the scales of justice to help a Servicemember accused of war crimes.

Second, when the President ordered the Navy to reverse Gallagher's demotion, he committed "a shocking and unprecedented intervention in a low-level review," according to Spencer.[82] After the trial, Gallagher requested to retire from the military; his court-martial conviction and sentence required the Navy to determine his rank at retirement and the characterization of his discharge from the Service.[83] These administrative issues are usually left to the military to sort out and do not warrant a commander in chief's time or attention. Again, as President, Mr. Trump probably had the authority to commute Gallagher's sentence—that is, to reduce the severity of the punishment.[84]

The President's third and final intervention in the Gallagher case may have been the most problematic from a civil-military relations perspective. When President Trump learned about the Navy's plan to put Gallagher before a Trident Review Board, he tweeted his disapproval. After Secretary Spencer resigned, the President expressed his dissatisfaction with the military's handling of the Gallagher case: "I was not pleased with the way that Navy Seal Eddie Gallagher's trial was handled by the Navy. He was treated very badly but, despite this, was completely exonerated on all major charges."[85]

In a very public fashion, the President excoriated an entire branch of the Armed Forces and prevented the Navy from holding an otherwise routine administrative board. To be sure, the Navy's criminal prosecution of Gallagher was not beyond reproach.[86] In fact, the case was part of the basis for then-Secretary Spencer's decision to order a comprehensive review of the Navy Judge Advocate General and Marine Corps Staff Judge Advocate organizations.[87] But the Navy's missteps in prosecuting the case did not warrant such high-level interference in a low-level administrative process.

Even more concerning, President Trump's intervention in the Navy's Trident Review Board undermined the

top SEAL commander, Rear Admiral Collin Green.[88] Rear Admiral Green had made it a priority in his command to stop the SEAL community's drift from Navy core values of honor, courage, and commitment.[89] By preventing the SEALs from convening an administrative board, the President's actions reportedly "angered many senior military officers and Pentagon civilians" and undercut the efforts of Rear Admiral Green to address ethical and disciplinary issues within his command.[90]

The Gallagher case alone risked eroding trust between senior military leaders and the President. With each intervention in the case, President Trump seemed to vindicate Cohen's theory of unequal dialogue in that the President received the advice and recommendations of his military advisors and decided to go in a different direction. Here, though, the cost of an unequal dialogue may prove to be too high and seems likely to degrade trust between the President and the military.[91] And, as political scientist Peter Feaver has observed: "Trust is the essential ingredient for healthy civil-military relations."[92]

Normative Arguments Against the Military Pardon Cases

The second and perhaps most damning criticism of the military pardon cases, broadly speaking, accused President Trump of being a "war crimes President."[93] This line of criticism factors in the President's previous remarks about the use of torture[94] and warfighting.[95] Critics have argued that the military pardons furnish further evidence that President Trump does not understand the law of war or the military he leads.

Although President Trump has made controversial remarks about torture and the conduct of war, his comments reveal something more fundamental than just bluster and bloviation. Rather, the rhetoric sheds insight into his underlying worldview and the reasons he issued pardons to Behenna, Lorance, Golsteyn, and Gallagher. To better understand the President's aggressive views about warfighting, we must know something about the Jacksonian tradition in

U.S. Air Force General Paul J. Selva, former Vice Chairman of the Joint Chiefs of Staff, departs after speaking to students enrolled in Advanced Ethics Counselor course in Air Force Judge Advocate General's School, at Maxwell Air Force Base, Alabama, April 30, 2019 (DOD/James K. McCann)

American politics—a tradition that traces its heritage back to the sixth President of the United States, Andrew Jackson.[96] The Jacksonian tradition helps explain President Trump's rationale for pardoning Behenna, Lorance, Golsteyn, and Gallagher, why his supporters endorsed his actions, and why some critics vehemently opposed the pardons.

The Jacksonian Tradition and the Trump Presidency. When Walter Russell Mead first described the Jacksonian tradition in 1999, he posited that it would "continue to enjoy major influence over both foreign and domestic policy in the United States for the foreseeable future."[97] With the ascendance of Donald Trump to the U.S. Presidency, Mead's prognostication could not have been more prescient. As a candidate and as President, Mr. Trump has spoken "directly to Jacksonian principles of populism, individualism, honor, and courage."[98]

Space constraints forbid a full panorama of Jacksonianism. The picture would be incomplete, though, without juxtaposing the Jacksonians with their distant cousins, the Jeffersonians.[99] Fortunately, Mead tidily distinguishes the two schools of thought this way: "Jeffersonians join the American Civil Liberties Union; Jacksonians join the National Rifle Association."[100] On foreign policy, Mead asserts that Jeffersonians are more dovish, while Jacksonians are "the most consistently hawkish."[101] During Vietnam, Mead loosely characterizes Jeffersonians as being among those who dodged the draft and "sought exemptions and substitutes," whereas Jacksonians, as they always have, "soldiered on, if sometimes bitterly and resentfully."[102]

Jacksonian hawkishness extends to views on the conduct of war. Jacksonians believe fundamentally "that wars must be fought with all available force."[103] They

are distrustful of international law and institutions and hew to an honor code that extends favorable treatment to those who live by the same.[104] "But," as Mead notes, "those who violate the code—who commit terrorist acts in peacetime, for example—forfeit its protection and deserve no consideration."[105] Honorable enemies get treated honorably; dishonorable enemies, such as IS and al Qaeda fighters, get treated as they deserve.[106]

Jacksonians "formed the core of Trump's passionately supportive base."[107] His brand of "populist nationalism" tapped into what Mead characterizes as a "truly surging force in American politics."[108] This surging force embraces "Jacksonian conceptions of 'honor,' as the Islamic State constitutes an inherently dishonorable adversary justifying the deployment of all and any means to destroy them."[109]

A final and important point about the Jacksonian tradition concerns its

Andrew Jackson, Thomas Sully, 1825 (Library of Congress/Detroit Publishing Company)

illuminates President Trump's philosophy about warfighting generally and explains why he supported Behenna, Lorance, Golsteyn, and Gallagher. His Jacksonian orientation diverges from cosmopolitan beliefs about limited war, international institutions, and application of international law during jus in bello. "When our soldiers have to fight for our country," President Trump has stated, "I want to give them the confidence to fight."[113] For critics of the war crime pardons, however, the confidence to fight does not necessitate or contemplate warfighting that deviates from the law of war.

The war crime pardons serve as a notable flashpoint in the country's continuing conversation about the way Americans fight and win wars, specifically, and the conduct of foreign policy, generally. Where one comes down on the military pardons cases likely depends on his or her ideological proximity to or distance from Jacksonian principles. The debate between Jacksonians and everyone else will almost certainly continue even after the Trump Presidency ends, but the criticism of the military pardon cases may have more to do with the Jacksonian view of warfighting than with President Trump per se. President Trump is, after all, a blunt, charismatic, and forceful manifestation of a venerable American tradition, not its progenitor. The beef, then, for many critics of the military pardons is with the underlying beliefs that brought them to President Trump's attention and compelled him to act.

"Just Cause" as a Related Explanation for War Crime Pardons. A distinct, yet related, explanation for President Trump's actions in the Behenna, Lorance, Golsteyn, and Gallagher cases concerns his views about the military's mission to eliminate or reduce the terrorist threat against the United States. The question arises whether Jacksonian support for aggressive warfighting and unconditional surrender equates to public forbearance of war crimes committed by U.S. Servicemembers. Available research suggests an affirmative answer.

A recent study by researchers Scott Sagan and Benjamin Valentino found, among other things, that "Americans

instinctive support of the military.[110] The degree of support for the military allows Jacksonians to recognize that Servicemembers "on the frontlines protecting society sometimes make mistakes."[111] As Mead succinctly explains, Jacksonians, such as President Trump, firmly believe that it is "unfair and even immoral" for warriors to risk their lives only to have "their choices second-guessed by armchair critics."[112] The Jacksonian tradition, therefore,

were . . . much more willing to describe soldiers who participate in unambiguous war crimes as behaving ethically when they were fighting for a just cause than when they were fighting for an unjust cause."[114] Sagan and Valentino presented a group of subjects with a story about a country's just counterattack, but with the added detail of war crimes. Particularly, the "just" side reportedly massacred 48 women and children.[115] Subjects exposed to this scenario were twice as willing to describe soldiers' war crimes as ethical when committed as part of a just cause.[116]

Sagan and Valentino's research design did not parse subjects by partisan political affiliation or ideology. Additional research could investigate whether Jacksonian-Trumpian adherents are more likely to excuse grave atrocities in service of a just cause.[117] But, as Sagan and Valentino concluded, many Americans "are willing to overlook acts of gratuitous killing by soldiers whose cause they believe to be just."[118] Along with Mead's argument that Jacksonians are unwilling to extend honor to dishonorable enemies, this finding suggests that President Trump's worldview envisions Servicemembers fighting with much more leeway against a hated enemy—a position that presumably would find currency among the President's most ardent supporters.

Finally, moral licensing may further explain why President Trump and many Americans give soldiers the benefit of the doubt when they perceive the military mission as just.[119] Sagan and Valentino define *moral licensing* as "the tendency of individuals to allow past moral behavior to excuse subsequent immoral behaviors."[120] Recall an instinctive support for the military among Jacksonians, and it becomes more evident why they would tend to excuse, overlook, or explain away crimes committed by Servicemembers on battlefields half a world away.

Against the backdrop of the Jacksonian tradition, President Trump's support for frontline troops and disgust for the Nation's enemies further explain why the commander in chief picked up on these particular cases and why, philosophically and politically, he decided to intervene in them. Moral licensing

coupled with Jacksonian fealty to the military could explain in part why President Trump and others were willing to see the actions of Behenna, Lorance, Golsteyn, and Gallagher in a more favorable light than did the journalists, academics, and retired military leaders who criticized the President's decisions regarding these actions.

Of course, the Jacksonian orientation does not inoculate the President's interventions in military justice against criticism. The Jacksonian tradition merely offers an ideological, as opposed to a political, explanation for President Trump's actions. Criticism of the military pardons seemed to dwell on President Trump as a leader, when the greater cause for concern may be the school of thought that undergirds his views about warfighting. The real and unsettled issue, then, is whether the United States wants to fight a war with a Jacksonian or someone else—because the choice is consequential for how Americans fight and how they treat their enemies.

Recommendations

Improve Law of War Guidance and Training. While discussing Richard Spencer's resignation with the press, Secretary of Defense Esper remarked, "The case of Eddie Gallagher has dragged on for months, and it's distracting too many. It must end."[121] When asked about Gallagher, Chairman of the Joint Chiefs of Staff General Mark Milley stated, "The case is now, in my view, closed."[122] The cases of Behenna, Lorance, Golsteyn, and Gallagher are indeed closed, legally, but the ramifications of these cases deserve a full accounting within DOD.[123]

After Spencer's abrupt resignation, Secretary Esper directed DOD general counsel to "review how the department educates and train [its] Servicemembers about wartime ethics and laws of armed conflict."[124] The review will entail "how the department monitors, investigates, reports, and adjudicates its adherence to the laws of armed conflict."[125] This review is a meaningful and needed first step toward improving the way DOD implements the law of war in light of the military pardons cases.[126]

When the general counsel completes the review, Secretary Esper should share the findings and recommendations with the Joint Chiefs of Staff. The review should serve as a launchpad for clearer and more robust uniform guidance about the law of war. The Services should then think anew about how they train on the law of war. Law of Armed Conflict (LOAC) training must occur more regularly and more intensively, similar to how the Services now conduct sexual assault and suicide prevention instruction. Servicemembers need more than just another judge advocate general briefing about LOAC; rather, they must be brought into the conversation about the principles of military necessity, humanity, proportionality, distinction, and honor. The Services should draw on the factual scenarios from the military pardon cases and other war crime cases in military history to invite Servicemembers to think more deeply about ethics and morality in the conduct of war.

Lastly, the military does not and should not train its members to be killing machines. Machines are emotionless, unfeeling, impartial, and impervious to the psychological trauma that can occur from killing another human being, even if that human being is an enemy. Servicemembers are not automatons; they are thinking and feeling social creatures. Americans should not want or expect them to kill unflinchingly, reflexively, impulsively, or wantonly. Why this should be so requires deeper thinking, from frontline warriors to strategic leaders, about discipline and self-control in the crucible of combat.

Congressional Review and Whistleblower Protections. Strategic leaders should welcome the ongoing congressional review of the military pardon cases.[127] They should be prepared to explain to Congress the law of war reforms they intend to implement. Military leaders will have to repeatedly remind and assure Congress that these cases are in no way being interpreted as a license to commit war crimes.

Senior military leaders must be prepared to delineate the protections afforded to whistleblowers who come

forward with allegations of war crimes.[128] A serious and unintended consequence of the military pardon cases is that Servicemembers may grow reluctant or unwilling to report war crimes for fear that their names will get dragged through the mud in the media.[129] The mechanisms for reporting war crimes must be clear and understandable to all Servicemembers, just as sexual assault reporting avenues have been strengthened and clarified in recent years.

Finally, Congress may want to review Presidential authority in the military justice process. Congress, of course, passes legislation governing the rules and regulations of the Armed Forces, and the UCMJ is the product of this congressional authority.[130] The commander in chief is an integral part of the military justice system.[131] That does not mean, however, that the President should have absolute authority to dictate any or all criminal or administrative dispositions within the military. Whether a President should have the power to stop something such as a Trident Review Board deserves further congressional scrutiny.

Conclusion

This essay has not resolved the debate whether President Trump should have pardoned the four Servicemembers for their war crimes. The essay's less lofty aim has been to contribute to the conversation about the military pardon cases through an objective assessment of two main ramifications flowing from them—namely, that Presidential meddling undermined the military justice system and thereby eroded trust between the military and the President, and that the pardons green-lighted a gloves-off approach to warfighting. As we have seen, the pardons cut many ways, paradoxically: They showed both healthy and unhealthy examples of civil-military relations, and they manifested through President Trump a persistent and venerable American philosophy about the conduct of war when waged against enemies perceived as dishonorable.

Returning to Captain Daniel's letter to President Nixon in 1971, the My Lai prosecutor not only expressed his dissatisfaction with the President's intervention in the Calley case but also conveyed astonishment at the public's backlash against the result of the trial. "For this nation to condone the acts of Lieutenant Calley," Captain Daniel wrote, "is to make us no better than our enemies."[132] Captain Daniel got it mostly right, but he missed a salient truth. For this nation to *condemn* the acts of Lieutenant Calley, or Lieutenant Behenna, Lieutenant Lorance, Major Golsteyn, or Chief Petty Officer Gallagher, it must first learn to tame the beast within that strains against its chains to bring unrelenting vengeance—even total war—to its enemies.[133] **JFQ**

Notes

[1] Richard Hammer, *The Court-Martial of Lt. Calley* (New York: Coward, McCann & Geoghegan, Inc., 1971), 50, 381–386.

[2] Chris Bray, *Court-Martial: How Military Justice Has Shaped America from the Revolution to 911 and Beyond* (New York: Norton, 2016), 337; Hammer, *The Court-Martial of Lt. Calley*, 17–18.

[3] Two days later, President Richard Nixon intervened in the case once again. This time, he announced that "[b]efore any sentence took effect . . . he would personally review the whole matter and decide whether the judges had come to the right sentence or whether he would reduce it." Hammer, *The Court-Martial of Lt. Calley*, 380. William Calley would remain under house arrest until his parole in 1974, after being convicted and sentenced for mass murder. Bray, *Court-Martial*, 338.

[4] Hammer, *The Court-Martial of Lt. Calley*, 385.

[5] Some commentators have labeled the four cases collectively, and somewhat imprecisely, as the "war crime cases" or the "war-crime pardons." For example, Andrew M. Bell and Thomas Gift, "War Crime Pardons and What They Mean for the Military," *War on the Rocks*, December 5, 2019, available at <https://warontherocks.com/2019/12/war-crime-pardons-and-what-they-mean-for-the-military/>; Kori Schake, "Trump's War-Crime Pardons Undermine the Military," *Defense One*, November 17, 2019, available at <www.defenseone.com/ideas/2019/11/trump-pardons-war-criminals/161354/>. However, the four Servicemembers were not charged with "war crimes" or "law of war" violations under international law, domestic law, or the Uniform Code of Military Justice (UCMJ). Instead, and probably for sound prosecutorial reasons, the military elected in each case to charge the Servicemembers with "standard criminal violations" of the UCMJ. See Charlie Dunlap, "No, the 'Laws of War' Are Not 'History,'" *Lawfare*, November 18, 2019, available at <https://sites.duke.edu/lawfire/2019/11/18/no-the-laws-of-war-are-not-history/>. Still, "war crimes" aptly and concisely describe the offenses underlying the four cases. For ease of description, this article at times uses the term *war crime* in a nontechnical, nonlegal sense as shorthand. For the most part, though, the author refers to the four cases collectively as the *military pardon cases*.

[6] Dan Lamothe and Josh Dewey, "'Insurgents' Lobbied Trump for War Crimes Pardons with Little Pentagon Involvement, Officials Say," *Washington Post*, November 21, 2019, available at <www.washingtonpost.com/national-security/insurgents-lobbied-trump-for-war-crimes-pardons-with-little-pentagon-involvement-officials-say/2019/11/21/b6a0c62e-0c75-11ea-bd9d-c628fd48b3a0_story.html>.

[7] These four were not the only Servicemembers to receive pardons from President Donald Trump. In 2018, he pardoned ex-Sailor Kristian Saucier, who had been convicted in Federal District Court for unlawfully retaining photographs he took of classified areas on a nuclear submarine. See Ryan Lucas, "Trump Pardons Ex-Navy Sailor Sentenced for Photos of Submarine," National Public Radio (NPR). March 9, 2018, available at <https://www.npr.org/2018/03/09/592440282/trump-pardons-ex-navy-sailor-sentenced-for-photos-of-submarine>.

[8] Andrew Exum, "How to Really Honor the Troops," *Defense One*, May 13, 2019, available at <www.defenseone.com/ideas/2019/05/how-really-honor-troops/156950/?oref=d-skybox?oref=d1-related-article>; Schake, "Trump's War-Crime Pardons Undermine the Military"; Elliot Ackerman, "President Trump's Pardons of Soldiers Show How Little He Knows About War," *Time*, November 18, 2019, available at <https://time.com/5731655/trumps-pardons-soldiers-war/>; Pauline M. Shanks Kaurin and Bradley J. Strawser, "Disgraceful Pardons: Dishonoring Our Honorable," *War on the Rocks*, November 25, 2019, available at <https://warontherocks.com/2019/11/disgraceful-pardons-dishonoring-our-honorable/>; "What Powers Does Trump Have as Commander in Chief?" *Morning Edition*, NPR November 26, 2019, available at <https://www.npr.org/2019/11/26/782867266/what-powers-does-trump-have-as-commander-and-chief>; Peter Feaver, "Trump Battled the Navy. Here Are the Casualties," *Foreign Policy*, November 26, 2019, available at <https://foreignpolicy.com/2019/11/26/trump-gallagher-case-navy-seal-war-crimes-casualties-spencer/>; Andrew Sullivan, "Donald Trump Is the War Crimes President," *New York Magazine*, January 10, 2020, available at <https://

nymag.com/intelligencer/2020/01/andrew-sullivan-donald-trump-is-the-war-crimes-president.html>; Martin Dempsey, Twitter post, May 21, 2019, 8:15 a.m., available at <https://twitter.com/Martin_Dempsey/status/1130809276191035392>; Barry McCaffrey, "Pardoning Convicted Troops Would Tell the World America No Longer Has a Disciplined Military," *Washington Post*, May 24, 2019, available at <www.washingtonpost.com/opinions/pardoning-convicted-troops-would-tell-the-world-america-no-longer-has-a-disciplined-military/2019/05/24/f289fbf2-7e3a-11e9-a5b3-34f3edf1351e_story.html>; James Stavridis, "We Trust the Navy SEALs to Protect America. Trump Should Trust the Navy SEALs to Judge Themselves," *Time*, November 25, 2019, available at <https://time.com/5739037/navy-seals-trump-trust/>; "Gen. Krulak Statement on Trump's Military Pardons," *Human Rights First*, November 15, 2019, available at <https://www.human-rightsfirst.org/press-release/gen-krulak-statement-trumps-military-pardons>.

[9] Stephen W. Preston, *Department of Defense* [DOD] *Law of War Manual* (Washington, DC: Office of the General Counsel, June 2015, updated December 2016), ii. The manual defines the *law of war* this way: "The *law of war* is that part of international law that regulates the resort to armed force; the conduct of hostilities and the protection of war victims in both international and non-international armed conflict; belligerent occupation; and the relationships between belligerent, neutral, and non-belligerent States." The manual also explains that the "*law of war* is often called *the law of armed conflict*." This essay uses *law of war* and *law of armed conflict* interchangeably, but both terms refer to jus in bello: "justice in war." See Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 5th ed. (New York: Basic Books, 2015), 21.

[10] "Statement of the Press Secretary Regarding Executive Clemency for Michael Behenna," The White House, May 6, 2019, available at <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-regarding-executive-clemency-michael-behenna/>.

[11] "Statement from the Press Secretary," The White House, November 15, 2019, available at <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-97/>.

[12] Andrew Dyer, "All the SEAL's Men: The Fox News Campaign That Made Eddie Gallagher Untouchable," *San Diego Tribune*, November 29, 2019, available at <www.sandiegouniontribune.com/news/military/story/2019-11-29/all-the-seals-men-the-fox-news-campaign-that-made-eddie-gallagher-untouchable>; Lamothe and Dewey, "'Insurgents' Lobbied Trump for War Crimes Pardons with Little Pentagon Involvement, Officials Say."

[13] Scott D. Sagan and Benjamin A. Val-entino, "Do Americans Approve of Trump's Pardons for Court-Martialed Military Officers?" *Washington Post*, December 16, 2019, available at <www.washingtonpost.com/politics/2019/12/16/do-americans-approve-trumps-pardons-court-martialed-military-officers/>. In their YouGov survey, Sagan and Valentino used the Clint Lorance case because they believed it was "the most clear-cut case in the recent pardons" because a court-martial had found Lorance guilty of second-degree murder. Overall, Sagan and Valentino reported that 41 percent of survey subjects approved of the pardon and 59 percent did not.

[14] *United States v. Behenna*, 71 M.J., 228, 231 (United States Court of Appeals for the Armed Forces 2012), available at <https://www.armfor.uscourts.gov/newcaaf/opinions/2011SepTerm/12-0030.pdf>.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid., 229.

[19] Ibid., 234–235. A second issue raised on appeal addressed whether the government failed to disclose exculpatory or favorable information to Behenna's trial defense attorneys. A government expert told the prosecutors that the theory presented by defense experts was plausible. After First Lieutenant Behenna testified, the same government expert determined he was telling the truth. Before leaving the trial, the expert told defense counsel that he would have been a great witness for them. Neither the trial court nor appellate courts granted relief to Behenna on this particular issue.

[20] Charlie Dunlap, "The Behenna Pardon: Some Answers (and Much More!)," *Lawfare*, May 19, 2019, available at <https://sites.duke.edu/lawfire/2019/05/19/the-behenna-pardon-some-answers-and-much-more/>.

[21] "Statement of the Press Secretary Regarding Executive Clemency for Michael Behenna."

[22] Ibid. For a more detailed discussion of the facts and legal issues in Behenna's case, see Kali Borkoski, "The Story of Michael Behenna and Mad Dog 5: 'Self Defense' in War," *SCOTUS*, May 29, 2013, available at <www.scotusblog.com/2013/05/the-story-of-michael-behenna-and-mad-dog-5-self-defense-in-war/>.

[23] "Statement of the Press Secretary Regarding Executive Clemency for Michael Behenna."

[24] Ibid.

[25] The following discussion of the Lorance case is from *United States v. Lorance*, ARMY 20130679, 2017 CCA LEXIS 429 (unpublished opinion), 2–13, available at <https://www.jagcnet.army.mil/Apps/ACCAOpinions/ACCAOpinions.nsf/MODD/331E0265D-C59E54F8525814E006BA1DC/%24FILE/mo-lorance,%20ca.pdf>.

[26] U.S. Department of the Army, *Crim-inal Investigation Division (CID) Report of Investigation* (Fort Bragg, NC: U.S. Army Criminal Investigation Command [redacted FOIA version], November 27, 2013), 000035. Dan Lamothe, "See Document Excerpts in the Army's War Crimes Case Against a Green Beret Hero," *Washington Post*, May 19, 2015, available at <www.washingtonpost.com/news/checkpoint/wp/2015/05/19/see-document-excerpts-in-the-armys-war-crimes-case-against-a-green-beret-war-hero/>. Lamothe posted the redacted Mathew Golsteyn investigation report on May 15, 2015, at <www.scribd.com/doc/265668561/Golsteyn-Army-CID-investigation?secret_password=PNNptwfNQ2XM-sAsZqkBF>.

[27] *CID Report*.

[28] Ibid.

[29] Ibid.

[30] Ibid. Also, while held in detention by U.S. forces, the murdered victim had seen the witness against him. According to Golsteyn, the witness feared that the victim would kill him and his family if released from detention.

[31] Dan Lamothe, "Inside the Stunning Fall and War-Crimes Investigation of an Army Green Beret War Hero," *Washington Post*, May 19, 2015, available at <www.washingtonpost.com/news/checkpoint/wp/2015/05/19/inside-the-stunning-fall-and-war-crimes-investigation-of-an-army-green-beret-war-hero/>.

[32] Ibid. In 2015, an Army Board of Inquiry (not a court-martial or criminal tribunal) did not substantiate the allegation that Golsteyn violated the Law of Armed Conflict, but nonetheless recommended his discharge from the Army with a General (Under Honorable Conditions) characterization for engaging in conduct unbecoming an officer and a gentleman. See Dan Lamothe, "Former Green Beret War Hero, Investigated in Killing, Survives Army Hearing with His Benefits," *Washington Post*, June 29, 2015, available at <www.washingtonpost.com/news/checkpoint/wp/2015/06/29/former-green-beret-war-hero-investigated-in-killing-survives-army-hearing-with-his-benefits/>.

[33] Dan Lamothe, "Army Reopens Probe into Suspected Bombmaker's Death After Special Forces Soldier's Fox News Interview," *Washington Post*, December 8, 2016, available at <www.washingtonpost.com/news/checkpoint/wp/2016/12/08/army-reopens-investigation-of-special-forces-soldier-accused-of-killing-unarmed-detainee/>.

[34] Barnini Chakraborty and Jennifer Griffin, "Army Opens Probe into Green Beret, Detainee's Death After FNC Interview," Fox News, December 9, 2016, last modified January 12, 2017, available at <www.foxnews.com/politics/army-reopens-probe-into-green-beret-detainees-death-after-fnc-interview>.

[35] Lamothe, "Army Reopens Probe into Suspected Bombmaker's Death After Special Forces Soldier's Fox News Interview."

[36] "Statement from the Press Secretary."

37 Dave Philipps, "Who Is Eddie Gallagher, the SEAL the Navy Wants to Expel?" *New York Times*, November 24, 2019, available at <www.nytimes.com/2019/11/24/us/edward-gallagher-navy-seals-trump.html?action=click&module=RelatedLinks&pgtype=Article>.

38 The following discussion of the Eddie Gallagher case is from "The Gallagher Effect," *The Weekly*, season 1, episode 23, December 27, 2019, available at <www.hulu.com/watch/330e9ea3-7aa9-439d-b206-f33b6487a9c3?>. Subscription required to view.

39 Philipps, "Who Is Eddie Gallagher, the SEAL the Navy Wants to Expel?"

40 George Petras, "Timeline: How Trump Intervened in the Navy SEAL Eddie Gallagher's War Crimes Case," *USA Today*, November 28, 2019, available at <www.washingtonpost.com/context/read-navy-secretary-richard-spencer-s-letter-to-president-trump/2bf70c2a-f811-43be-9e21-b02f1fe54a26/>. Gallagher was also "accused of firing a sniper rifle at civilians, striking a girl wearing a flower-print hijab as she walked along a riverbank and an old man carrying a water jug," but was acquitted of those allegations. Philipps, "Who Is Eddie Gallagher, the SEAL the Navy Wants to Expel?"

41 "The Gallagher Effect," clip approx. at 14:56.

42 Ibid., clip approx. at 15:14. The UCMJ does not allow for a bail system; instead, commanders can order Servicemembers accused of military crimes into confinement while they await trial only after certain criteria are met and a hearing is held. See Part II, Chapter II, "Rule 305, Pretrial Confinement," 305(a)-(m), in *Manual for Courts-Martial, United States* (Washington, DC: Department of Defense), II-22–II-27.

43 Dyer, "All the SEAL's Men."

44 Donald J. Trump, Twitter post, March 30, 2019, 8:14 a.m., available at <https://twitter.com/realdonaldtrump/status/1111965027483951105>. President Trump tweeted, "In honor of his past service to our Country, Navy Seal #EddieGallagher will soon be moved to less restrictive confinement while he awaits his day in court. Process should move quickly! @foxandfriends@RepRalphNorman."

45 Philipps, "Who Is Eddie Gallagher, the SEAL the Navy Wants to Expel?"

46 Ibid.

47 Petras, "Timeline." The sentence also included four months' confinement, but Gallagher received credit for time already served before trial, meaning he walked out of the courthouse a free man.

48 "Statement from the Press Secretary."

49 Ibid. The relevant portion reads, "Today, President Donald J. Trump signed . . . an order directing the promotion of Special Warfare Operator First Class Edward R. Gallagher to the grade of E-7, the rank he held before he was tried and found not guilty of nearly all of the charges against him."

50 Carl Prine, "Navy Secretary Backs Admirals in Tussle with Trump over SEAL Trident, Report Says," *Navy Times*, November 22, 2019, available at <www.navytimes.com/news/your-navy/2019/11/23/report-navy-secretary-backs-admirals-in-tussle-with-trump-over-seal-trident/>.

51 Donald J. Trump, Twitter post, November 21, 2019, 8:30 a.m., available at <https://twitter.com/realdonaldtrump/status/1197507542726909952?lang=en>.

52 Richard Spencer, "I Was Fired as Navy Secretary. Here's What I've Learned Because of It," *Washington Post*, November 27, 2019, available at <www.washingtonpost.com/opinions/richard-spencer-i-was-fired-as-navy-secretary-heres-what-ive-learned-because-of-it/2019/11/27/9c2e58bc-1092-11ea-bf62-eadd5d11f559_story.html>.

53 Ibid.

54 "Remarks by Secretary Esper in a Press Gaggle," Department of Defense, November 25, 2019, available at <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2026000/remarks-by-secretary-esper-in-a-press-gaggle/>; Richard V. Spencer, Letter to President Trump, *Washington Post*, November 24, 2019, available at <www.washingtonpost.com/context/read-navy-secretary-richard-spencer-s-letter-to-president-trump/2bf70c2a-f811-43be-9e21-b02f1fe54a26/>.

55 "Remarks by Secretary Esper in a Press Gaggle."

56 Petras, "Timeline."

57 Understandably, civilian and uniformed military leaders have not revealed the particular advice and recommendations they gave to the President about the military pardon cases. But their public comments coupled with concomitant reporting suggest they advised the President against intervening. See Lamothe and Dewey, "'Insurgents' Lobbied Trump for War Crimes Pardons with Little Pentagon Involvement, Officials Say"; "Remarks by Secretary Esper in a Press Gaggle"; "ICYMI: Rep. Moulton Grills Military's Most Seniors Leaders on Trump's Pardons, Retreat from Iran Deal," December 13, 2019, available at <https://moulton.house.gov/press-releases/icymi-rep-moulton-grills-militarys-most-seniors-leaders-on-trumps-pardons-retreat-from-iran-deal>; Meghann Myers, "Esper: 'Robust' Conversation with Trump About Proposed Pardons for SEAL, Two Soldiers," *Military Times*, November 6, 2019, available at <www.militarytimes.com/news/your-military/2019/11/06/esper-will-ask-trump-to-reconsider-pardons-for-service-members-charged-with-convicted-of-war-crimes-report-says/>.

58 Peter D. Feaver, "The Civil-Military Problematique: Huntington, Janowitz, and the Question of Civilian Control," *Armed Forces & Society* 23, no. 2 (Winter 1996), 160, available at <https://journals.sagepub.com/doi/10.1177/0095327X9602300203>.

59 Ibid., 158.

60 Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge: Belknap Press of Harvard University Press, 1957), 84.

61 Ibid.

62 Ibid.

63 Ibid.

64 Eliot Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime* (New York: Anchor Books, 2003), 4.

65 Ibid., 208–209.

66 Ibid., 209.

67 U.S. Const., Art. 2, § 2, cl. 1.

68 "Submission of Petition; Form to Be Used; Contents of Petition," 28 C.F.R. § 1.1 2020, available at <https://www.law.cornell.edu/cfr/text/28/1.1>.

69 Gallagher, likewise, had been tried, convicted, and sentenced when he received his executive clemency. As we have seen, though, the President also intervened in the case before trial, and intervened once more *after* restoring Gallagher's rank. For these reasons, his case is distinguishable from the others, procedurally.

70 The Web site for the Department of Justice's Office of the Pardon Attorney includes a section for frequently asked questions. One question asks whether the President can issue a pardon before someone has been indicted, convicted, or sentenced. The response is that "it would be highly unusual," but notes that President Gerald Ford, President Jimmy Carter, and President George H.W. Bush issued pardons outside of the customary sequence. See Department of Justice, Office of the Pardon Attorney, available at <https://www.justice.gov/pardon/frequently-asked-questions>.

71 Ibid.

72 John Wagner, "Trump Says Pardoning War Criminals 'a Little Bit Controversial,' Suggests Delay in Deliberations," *Washington Post*, May 24, 2019.

73 For example, the President of the United States is authorized to convene courts-martial under Article 22, UCMJ (10 USC § 22).

74 "Remarks by Secretary Esper in a Press Gaggle."

75 By "relatively unscathed," the author means that Major Golsteyn avoided a trial and possible sentence to confinement, unlike Lorance and Behenna. Golsteyn did endure a lengthy criminal investigation, a board of inquiry, and other collateral consequences, which continued after his pardon. Even after being pardoned, the Army denied Golsteyn's request to be reinstated into the Green Berets. See Dave Philipps, "Army Denies Request by Soldier Pardoned by Trump, Setting Up Showdown," *New York Times*, January 9, 2020, available at <www.nytimes.com/2020/01/09/us/mathew-golsteyn-army-war-crime.html>.

76 Dyer, "All the SEAL's Men."

77 Spencer, "I Was Fired as Navy Secretary."

78 David Ignatius, "Trump's Meddling in a SEAL Disciplinary Case Risks a Collision with the Navy," *Washington Post*, November

21, 2019, available at <www.washingtonpost.com/opinions/trump-is-sabotaging-his-military/2019/11/21/6b46199e-0cad-11ea-97ac-a7ccc8dd1ebc_story.html>.

[79] Rules for Court-Martial 304 and 305, in *Manual for Courts-Martial*, are touchstones for a President's authority to change the conditions of confinement for a military member. As President Nixon weighed options in the Calley case, he reportedly rejected the advice of White House Counsel John Dean. Dean argued that the President "could not exercise piecemeal the powers of a court-martial convening authority." Furthermore, "Dean considered it unwise for the President to take some action as a convening authority because this would make him the convening authority for all future aspects of the case." See Michal R. Belknap, *The Vietnam War on Trial: The My Lai Massacre and Court-Martial of Lieutenant Calley* (Lawrence: University Press of Kansas, 2002), 197–199. In Gallagher's case, President Trump appears to have withheld a military commander's authority and directed a lesser form of restriction. But had Gallagher committed an additional offense prior to trial, but after the President's order, it seems unlikely, yet not improbable, that the commander in chief would have wanted to referee a request to return Gallagher to more restrictive confinement.

[80] David Martin, "Eddie Gallagher, Navy SEAL Acquitted of Stabbing Wounded ISIS Prisoner to Death, Tells His Story," CBS News, March 1, 2020, available at <www.cbsnews.com/news/eddie-gallagher-navy-seal-isis-prisoner-60-minutes-interview-2020-03-01/>. After the court-martial, President Trump congratulated Gallagher, tweeting, "Congratulations to Navy Seal Eddie Gallagher, his wonderful wife Andrea, and his entire family. You have been through much together. Glad I could help!" Donald J. Trump, Twitter post, July 3, 2019, 10:47 a.m., available at <https://twitter.com/realDonaldTrump/status/1146430380981067777>.

[81] Spencer, "I Was Fired as Navy Secretary."

[82] Ibid.

[83] Ibid.

[84] According to the Department of Justice's Office of the Pardon Attorney, commutation "reduces a sentence, either totally or partially, that is then being served, but it does not change the fact of conviction, imply innocence, or remove civil disabilities that apply to the convicted person as a result of the criminal conviction." Commutation typically reduces a person's prison sentence, but in Gallagher's case it had the effect of restoring his military rank. See Department of Justice, Office of the Pardon Attorney, available at <https://www.justice.gov/pardon/frequently-asked-questions>.

[85] Donald J. Trump, Twitter post, November 24, 2019, 6:32 p.m., available at <https://twitter.com/realdonaldtrump/status/1198746358091530241>.

[86] Carl Prine, "SECNAV Orders Compre-

hensive Review of Navy, Marine Corps JAGs," *Military Times*, August 22, 2019, available at <www.militarytimes.com/news/your-navy/2019/08/22/navsec-orders-comprehensive-review-of-navy-marine-corps-jags/>.

[87] Zachary D. Spillman, "SECNAV Orders a Review of the Navy and Marine Corps Legal Communities," *CAAFlog*, August 23, 2019, available at <www.caaflog.com/2019/08/23/secnav-orders-a-review-of-the-navy-and-marine-corps-legal-communities/>.

[88] Ignatius, "Trump's Meddling in a SEAL Disciplinary Case Risks a Collision with the Navy."

[89] Ibid. Rear Admiral Collin P. Green, Naval Special Warfare Command, to Major Commanders, Naval Special Warfare, memorandum, subject: Guidance from the Commander, August 20, 2019, available at <http://cdn.cnn.com/cnn/2019/images/08/23/radm.green.guidance.directive.pdf>.

[90] Ignatius, "Trump's Meddling in a SEAL Disciplinary Case Risks a Collision with the Navy."

[91] Morning Edition, "What Powers Does Trump Have as Commander in Chief?"

[92] Ibid. During this show, in the interview section, Feaver explains further: "But under the principle of civilian control, President Trump has the right to do these things. That doesn't make them right. He has the right to be wrong, in other words. But when a President exercises that right to be wrong on matters that the military care deeply about, the President tends to pay a price. And I do think there—the price will be paid in terms of a loss of trust between the military and the President. And that trust is the essential ingredient for healthy civil-military relations."

[93] Sullivan, "Donald Trump Is the War Crimes President"; Adam Serwer, "The War-Crimes President," *The Atlantic*, November 27, 2019, available at <www.theatlantic.com/ideas/archive/2019/11/trump-war-crimes/602731/>.

[94] Jenna Johnson, "Donald Trump on Waterboarding: 'If It Doesn't Work, They Deserve It Anyway,'" *Washington Post*, November 23, 2015, available at <www.washingtonpost.com/news/post-politics/wp/2015/11/23/donald-trump-on-waterboarding-if-it-doesnt-work-they-deserve-it-anyway/>; Jenna Johnson, "Donald Trump on Waterboarding: 'Torture Works,'" *Washington Post*, February 17, 2016, available at <www.washingtonpost.com/news/post-politics/wp/2016/02/17/donald-trump-on-waterboarding-torture-works/>. As a Presidential candidate, Mr. Trump announced his support for killing the families of terrorists. See Tom LoBianco, "Donald Trump on Terrorists: 'Take Out Their Families,'" CNN, December 3, 2015, available at <www.cnn.com/2015/12/02/politics/donald-trump-terrorists-families/index.html>. More recently, President Trump suggested the United States could attack cultural heritage sites

inside Iran: ". . . targeted 52 Iranian sites (representing the 52 American hostages taken by Iran many years ago), some at a very high level & important to Iran & the Iranian culture, and those targets, and Iran itself, WILL BE HIT VERY FAST AND VERY HARD. The USA wants no more threats!" Donald J. Trump, Twitter post, January 4, 2020, 5:52 p.m., available at <https://twitter.com/realdonaldtrump/status/1213593975732527112>.

[95] Donald J. Trump, Twitter post, October 12, 2019, 9:49 a.m., available at <https://twitter.com/realdonaldtrump/status/1183016899589955584?lang=en>. The President tweeted, "The case of Major Mathew Golsteyn is now under review at the White House. Mathew is a highly decorated Green Beret who is being tried for killing a Taliban bombmaker. We train our boys to be killing machines, then prosecute them when they kill! @PeteHegseth."

[96] Walter Russell Mead, "The Jacksonian Tradition: And American Foreign Policy," *The National Interest*, no. 58 (Winter 1999/2000), 5–29, available at <https://www.jstor.org/stable/pdf/42897216.pdf>.

[97] Ibid., 9.

[98] Michael Clarke and Anthony Ricketts, "Donald Trump and American Foreign Policy: The Return of the Jacksonian Tradition," *Comparative Strategy* 36, no. 4 (2017), 367, available at <https://doi.org/10.1080/01495933.2017.1361210>.

[99] Besides Jacksonian and Jeffersonian traditions, Mead identifies the Hamiltonian and Wilsonian schools of thought as rounding out the overarching perspectives in American foreign policy. This essay focuses almost exclusively on the Jacksonian tradition, with an occasional nod toward the Jeffersonians.

[100] Mead, "The Jacksonian Tradition," 8. Mead further explains Jacksonianism as "less an intellectual or political movement than an expression of the social, cultural, and religious values of a large portion of the American public" (9). And Jacksonians rely on "an instinct rather than ideology—a culturally shaped set of beliefs and emotions rather than a set of ideas" (17).

[101] Ibid., 8.

[102] Ibid., 14.

[103] Ibid., 23.

[104] Ibid., 18.

[105] Ibid.

[106] Ibid., 21.

[107] Walter Russell Mead, "The Jacksonian Revolt: American Populism and the Liberal Order," *Foreign Affairs*, March/April 2017, 3, available at <www.foreignaffairs.com/articles/united-states/2017-01-20/jacksonian-revolt>.

[108] Ibid.

[109] Clarke and Ricketts, "Donald Trump and American Foreign Policy," 373.

[110] Mead, "Jacksonian Revolt," 5. Mead includes the police as being among the groups receiving instinctive support from Jacksonian voters.

[111] Ibid.

[112] Ibid.

[113] "Remarks by Secretary Esper in a Press Gaggle."

[114] Scott D. Sagan and Benjamin A. Valentino, "Just War and Unjust Soldiers: American Public Opinion on the Moral Equality of Combatants," *Ethics & International Affairs* 33, no. 4 (2019), 414, available at <https://doi.org/10.1017/S0892679419000431>. In their study, Sagan and Valentino constructed four hypothetical scenarios about a war between the fictional countries of "Eastland" and "Westeria" and assigned about 150 participants "to each condition and each subject read only one story." In each scenario, Sagan and Valentino varied an aspect of the conflict "to isolate the effects of beliefs about the justice of the war's cause on the public's ethical judgments about the conduct of combatants and the moral responsibility of leaders." Sagan and Valentino, "Just War and Unjust Soldiers," 420–421.

[115] Ibid., 444.

[116] Ibid., 427.

[117] Ibid., 433.

[118] Ibid., 432.

[119] Ibid., 433.

[120] Ibid.

[121] "Remarks by Secretary Esper in a Press Gaggle."

[122] Idrees Ali, "Navy SEAL Case Closed as Far as Top U.S. General Concerned," Reuters, November 25, 2019, available at <www.reuters.com/article/us-usa-military-seals-milley/navy-seal-case-closed-as-far-as-top-u-s-general-concerned-idUSKBN1XZ0ZZ>.

[123] According to some reporting, President Trump may be considering pardons for others convicted of war crimes. See Spencer Ackerman and Asawin Suebsaeng, "Justice Department Stonewalls Senate Democrats on Trump's War-Crimes Clemency," *The Daily Beast*, January 16, 2020, available at <www.thedailybeast.com/justice-department-stonewalls-senate-democrats-on-trumps-war-crimes-clemency>.

[124] "Remarks by Secretary Esper in a Press Gaggle."

[125] Ibid.

[126] John C. Dehn, "Why a President Cannot Authorize the Military to Violate (Most of) the Law of War," *William & Mary Law Review* 59, no. 3 (2018), 816, available at <https://scholarship.law.wm.edu/wmlr/vol59/iss3/3>.

[127] Ackerman and Suebsaeng, "Justice Department Stonewalls Senate Democrats on Trump's War-Crimes Clemency."

[128] DOD Directive (DODD) 2311.01E, *DOD Law of War Program*, February 22, 2011, 8. DODD 2311.01E, para. 6.3, mandates that "all military . . . personnel shall report reportable incidents" of war crimes through their chain of command. Later in the paragraph, the directive allows for reports to be made through other channels outside the chain of command. Servicemembers need to know their avenues for reporting war crimes, especially the agencies outside the chain of command eligible to receive a report. Junior members may feel reluctant to report a war crime through their chain of command, especially in circumstances where someone in the chain allegedly committed the act.

[129] Dave Phillips, "Navy Reduces Punishment for SEAL in War Crimes Case," *New York Times*, October 29, 2019, available at <https://www.nytimes.com/2019/10/29/us/navy-seal-gallagher-clemency.html?action=click&module=RelatedLinks&pgtype=Article>.

[130] U.S. Const., art. 1, § 8, cl. 14.

[131] For example, the President issues the Rules for Court-Martial and the Military Rules of Evidence that establish court-martial procedure.

[132] Hammer, *The Court-Martial of Lt. Calley*, 385. One poll "showed that nearly 80 per cent of Americans bitterly opposed the finding." Hammer, *The Court-Martial of Lt. Calley*, 374; see "Poll Finds Majority Think Calley Was a Scapegoat," *New York Times*, April 17, 1971, available at <www.nytimes.com/1971/04/17/archives/poll-finds-majority-think-calley-was-a-scapegoat.html>. Additionally, a separate 1971 Gallup/Newsweek poll found that 11 percent of Americans approved of the verdict. Sagan and Valentino, "Do Americans Approve of Trump's Pardons for Court-Martialed Military Officers?"

[133] Sagan and Valentino, "Just War and Unjust Soldiers," 435. Sagan and Valentino's article quotes George C. Marshall as stating, "Once an army is involved in war, there is a beast in every fighting man which begins tugging at its chains. And a good officer must learn early on how to keep the beast under control, both in his men and himself." George C. Marshall, quoted in Luke Mogelson, "A Beast in the Heart of Every Fighting Man," *New York Times*, April 27, 2011, available at <www.nytimes.com/2011/05/01/magazine/mag-01KillTeam-t.html>.

Air National Guard intelligence analysts assigned to 181st Intelligence Wing, 137th Intelligence Squadron Unclassified Processing, Assessment, and Dissemination site test new domestic response artificial intelligence technology at Hulman Field Air National Guard Base, Indiana, November 2, 2019 (U.S. Air National Guard/L. Roland Sturm)

Artificial Intelligence
A Decisionmaking Technology

By Mark M. Zais

Colonel Mark M. Zais, USA, wrote this essay while attending the U.S. Army War College. It won the Strategy Article category of the 2020 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

With the release of its first artificial intelligence (AI) strategy in 2019, the Department of Defense (DOD) formalized the increased use of AI technology throughout the military, challenging senior leaders to create "organizational AI strategies" and "make related resource allocation decisions."[1] Unfortunately, most senior leaders currently have limited familiarity with AI, having developed their skills in tactical counterinsurgency environments, which reward strength (physical and mental), perseverance, and diligence. Some defense scholars have advocated a smarter military, emphasizing intellectual human capital and arguing that cognitive ability will determine success in strategy development, statesmanship, and decisionmaking.[2] AI might complement that ability but cannot be a substitute for it. Military leaders must leverage AI to help them adapt and be curious. As innovative technologies with AI applications increasingly become integral to DOD modernization and near-peer competition, senior leaders' knowledge of AI is critical for shaping and applying our AI strategy and creating properly calibrated expectations.

War is about decisionmaking, and AI enables the technology that will transform how humans and machines make those decisions.[3] Successful use of this

general-purpose technology will require senior leaders who truly understand its capabilities and can demystify the hyperbole.[4] Within current AI strategy development and application, many practitioners have a palpable sense of dread as we crest the waves of a second AI hype cycle, seemingly captained by novices of the AI seas.[5] In-house technical experts find it difficult to manage expectations and influence priorities, clouded by buzzwords and stifled by ambitions for "quick wins." The importance of AI-related education increases with AI aspirations and the illusion of progress. Without that education, we face a world where senior leaders use AI-enabled technologies to make decisions related to national security *without* a full grasp of the tools that they—and our adversaries—possess. This would be equivalent to a combat arms officer making strategic military landpower decisions without the foundations of military education in maneuver warfare and practical experience.

Educating Senior Leaders in AI

Strategic decisionmaking in a transformative digital environment requires comparably transformative leadership. Modernization of the military workforce should parallel modernization of equipment and technology. In the short term, senior leaders require executive AI education that equips them with enough knowledge to distill problems that need AI solutions and that provides informed guidance for customized solutions. With the ability to trust internal expertise, the military can avoid overreliance on consultants and vendors, following Niccolò Machiavelli's warning against dependence on auxiliary troops.[6] In the long term, military education should give the same attention to AI that is provided to traditional subjects such as maneuver warfare and counterinsurgency operations. Each steppingstone of military education should incorporate subjects from the strategic domain, including maneuver warfare, information warfare, and artificial intelligence.

As the military becomes more AI-driven, it will become more quantitative and automated. The allure of AI has

encouraged rebranding of existing computing methodologies (for example, *neural networks* has become *deep learning*), which has been useful in attracting attention and funding.[7] Elevating the discourse of machine learning and deep learning to the senior leader level means domain knowledge must be elevated as well. This is critical when working with the private sector. For instance, when engaging with vendors or discussing machine learning applications, senior leaders should know what kind of machine learning (linear regression, logistic regression, decision trees, Naïve Bayes) is desired or already in use.

What does AI education look like for senior leaders? The definition of AI is gradually evolving and becoming broader. Today, almost any computerized system that solves a problem or informs a decision falls under the AI umbrella. The relationship between AI and data science is underpinned by a complex interdependence of many multidisciplinary skills and methods. As such, we cannot expect senior leaders to have a deep understanding of all the constituent AI disciplines and the continuously evolving technology. These leaders should, however, have broad enough knowledge to understand the relationships among data science, machine learning, and deep learning and to be familiar with the methods that each uses.

Senior leaders should also have similar understanding of the capabilities of related fields essential to AI solutions, such as data mining, data management, data architecture, and cloud computing.

Applying Knowledge to AI Strategy

To realize the potential of AI, senior leaders (both military and civilian) must make intellectual human capital central to DOD AI strategy. The level of AI knowledge that those senior leaders possess will determine their success in setting priorities in requirements and applying AI strategies. That will require a top-down AI strategy that is consistent with proven AI applications in industry. Three key indicators evince the progress of these leaders in achieving the mastery that their positions require.

First, they would stop searching for AI solutions to every problem. Business leaders identify the core business decisions they are trying to solve; likewise, military leaders should pinpoint critical decisions that affect an objective and assess the role that data play in those decisions. That analysis would show when the solution requires data-driven approaches, such as rule-based systems, advanced analytics, statistics, econometrics, optimization, simulation, machine learning, or deep learning—and when it does not. Knowledgeable leaders will accept that the best solution is not always an AI solution.

Second, they would manage expectations so as not to be trapped by a hype cycle that leads to disillusionment.[8] AI leaders need to understand that a return on investment will be slow and, perhaps, disappointing.[9] That will be particularly true when new applications are launched without needed supporting infrastructure and data architecture. That support may require multiple data sources, teams of people, and integration of data before the AI application can begin making predictions and evaluations. Knowledgeable leaders will understand the differences between expectations of deliverables for AI and those for information technology (IT). Whereas IT delivers known services, AI and data science engage in discovery, which is inherently unpredictable, unless a previously solved problem or previously used data is involved in the science. Like any discovery process, they may not produce desired solutions.

Third, senior leaders must build a workforce that supports AI to a scale needed to support the DOD enterprise. Military Services and subordinate organizations must transform their workforces to be proficient digital-data practitioners, able to leverage human-machine opportunities across all warfighting functions. An AI-ready workforce includes leaders who know about not only the domain but also the limits of their knowledge. That self-awareness will allow them to assemble internal staffs that have a deeper understanding of mathematical modeling needed to lead data scientists and engineers. These staff capabilities are critical

to building infrastructures and identifying manageable projects that can be benchmarked against existing ones. Complex organizations require four to five data engineers for every data scientist in order to create the data pipelines essential to the applications.[10] If senior leaders do not understand these needs, then they need senior advisors with that technical knowledge and training to converse with them.

How does the military scale its AI workforce to support the enterprise? Currently, large businesses struggle to hire enough data scientists. DOD faces the same challenge, with organizations as large and as geographically distributed as any global multinational corporation; however, assuming there is the top-level commitment of resources, acquiring and retaining qualified data personnel may seem more daunting than reality. Whatever the size of the organization, all projects start with a small team, which can then grow with the number and complexity of the problems addressed with AI. One industry expert has described the scaling issue like this: "A big company is a bunch of little people all working in a company."[11]

Conclusion

In some ways, the current evolution of AI is similar to the rapid growth of the DOD cyber community over the last decade. The mantra of "we need to do more AI" evokes comparisons to ambitious cyber goals that outpaced workforce growth and capabilities. In the case of cyber technology, military culture change was slow; leaders who had thrived under earlier, simpler rules and understanding for the world were criticized for neglecting the professional military education needed to achieve a high level of cyber conceptualization.[12] Time will tell whether the current DOD AI modernization strategy will yield similar results. There is no doubt that the warfighting environment is rapidly changing. AI, like information warfare and space, will require a commitment to the development of intellectual capital to ensure that the workforce and leadership are prepared to succeed in these fast-moving domains. The successful

adoption of AI technologies requires leaders who can direct the strategy— and not rely only on outside experts and DOD AI research centers. **JFQ**

Notes

[1] *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington, DC: Department of Defense, 2019), 14.

[2] Everett S.P. Spain, J.D. Mohundro, and Bernard B. Banks, "Intellectual Capital: A Case for Cultural Change," *Parameters* 45, no. 2 (Summer 2015), 77–91.

[3] Tom Upchurch, "How China Could Beat the West in the Deadly Race for AI Weapons," *Wired*, August 8, 2018, available at <https://www.wired.co.uk/article/artificial-intelligence-weapons-warfare-project-maven-google-china>.

[4] Wim Naudé, "AI's Current Hype and Hysteria Could Set the Technology Back by Decades," *The Conversation*, July 24, 2019, available at <https://theconversation.com/ais-current-hype-and-hysteria-could-set-the-technology-back-by-decades-120514>.

[5] Alok Aggarwal, "Resurgence of Artificial Intelligence During 1983–2010," *Scry Analytics*, January 20, 2018, available at <https://scryanalytics.ai/resurgence-of-artificial-intelligence-during-1983-2010>.

[6] Niccoló Machiavelli, *The Prince*, ed. and trans. David Wootton (Indianapolis: Hackett, 1995), chapter 13.

[7] Samira Pouyanfar et al., "A Survey on Deep Learning: Algorithms, Techniques, and Applications," *ACM Computing Surveys* 51, no. 5 (September 2018), available at <https://dl.acm.org/doi/pdf/10.1145/3234150>.

[8] Jackie Fenn and Marcus Blosch, "Understanding Gartner's Hype Cycles," *Gartner*, August 20, 2018, available at <www.gartner.com/en/documents/3887767/understanding-gartner-s-hype-cycles>.

[9] Sankar Narayanan, "How to Measure the ROI of AI," interview by Daniel Fraggella, *Artificial Intelligence in Industry*, December 3, 2019, podcast audio, 3:20, available at <https://emerj.com/artificial-intelligence-podcast>.

[10] Jesse Anderson, "Data Engineers vs. Data Scientists," *O'Reilly*, April 11, 2018, available at <www.oreilly.com/radar/data-engineers-vs-data-scientists/>.

[11] Charles Martin, "How to Get Started with an Effective AI Strategy," interview by Daniel Fraggella, *Artificial Intelligence in Industry*, June 28, 2019, podcast audio, 6:35, available at <https://emerj.com/artificial-intelligence-podcast>.

[12] Johnna T. Wynne, *Wired Fast and Thinking Slow: Cyber Technology and the U.S. Army* (Fort Leavenworth, KS: School of Advance Military Studies, 2016).

Captain Joseph O'Brien, mission commander of Task Force New York City, greets medical providers joining USNS *Comfort*, which is working with Javits New York Medical Station as integrated system to relieve city's medical system, in support of U.S. Northern Command's Defense Support of Civil Authorities as response to COVID-19 pandemic, April 15, 2020 (U.S. Navy/Scott Bigley)

Decision Superiority Through Joint All-Domain Command and Control

By Terrence J. O'Shaughnessy

General Terrence J. O'Shaughnessy, USAF (Ret.), most recently served as Commander, U.S. Northern Command and North American Aerospace Defense Command.

I have had the honor to lead both U.S. Northern Command (USNORTH-COM) and the binational North American Aerospace Defense Command (NORAD) for the past 2 years. During that time, the commands have undergone a critical transformation to ensure their collective ability to deter and defeat the very real threats posed by peer adversaries. In order to accomplish this no-fail homeland defense mission during a time of crisis, we must be able to perform a number of critical capabilities, which in their most distilled form are maintaining domain awareness, exercising command and control (C2) of assigned forces, and defeating adversary attacks. These capabilities are not new but rather have existed since each command's inception and have been key to providing a credible deterrent against our adversaries for many years.

While these critical capabilities for homeland defense may be enduring, the requirements needed to carry them out change over time. When I assumed

command of USNORTHCOM and NORAD (NC&N), it was clear that we needed to rapidly improve our capabilities to fulfill the sacred mission of defending the homeland. Our adversaries had adapted, operating across new domains with faster and more advanced weaponry designed to circumvent our aging defenses. To counter these weapons and operate at the speed of relevance today, we must have awareness across all-domain C2 providing a fused threat picture across subsurface, maritime, land, air, near-space, space, and cyber activities, and defeat mechanisms capable of neutralizing adversary attacks against our critical infrastructure. The linchpin between these two capabilities is Joint All-Domain Command and Control (JADC2).

What is JADC2? Describing and ultimately producing JADC2 has proved elusive for the Department of Defense (DOD) because, in part, it is difficult to translate an aspirational concept into a shared vision and then into programming requirements. One approach has been to describe JADC2 by its desired attributes. In that sense, we talk about a redundant and resilient architecture to enable faster and more reliable communications, or the ability to link fused sensor and reporting data to the best shooter in ways that flatten unnecessary organizational hierarchies, gaining the leverage needed to deny an enemy the ability to hold us at risk. While these descriptions are certainly useful, JADC2 may be best described by its ultimate purpose: *decision superiority.*

JADC2 is C2 for the digital age—the architecture needed to produce faster and better decisions for our warfighters from the tactical edge to the strategic leader. What makes JADC2 different from previous C2 constructs is that it is built on a data-rich foundation that employs the power of machines to enhance decisionmaking. This new capability moves beyond the limitations of human capacities to produce machine-enabled insights that can identify anomalous events, anticipate what will happen next, and generate options with associated repercussions and risks.

To illustrate, a recent Amazon Web Service Next Gen Stats commercial shows at a basic level what this capability could look like (see figure 1). The commercial demonstrates artificial intelligence (AI) analyzing National Football League (NFL) plays. It identifies what AI-enabled insights could do for the decisionmaker, in this case an NFL quarterback. Using AI, a coach could assess whether the risks are worth the reward when looking at the probability of a completion for a 7-yard first down versus a lower probability but higher payoff for a 53-yard touchdown.

Beyond this simple illustration is an even more robust potential when we factor in machine learning (ML) based on previous patterns of behavior, incorporating historical analysis with the current situation to anticipate the future. A quarterback such as Tom Brady approaches the line of scrimmage with a brain processing two decades of NFL experiential learning. He knows the defensive coordinator whom he is facing and his own patterns for any number of circumstances, giving him a pre-snap edge when he evaluates the scheme. What machine-enabled insights could do, if the information could be transmitted to the quarterback in real time, is replicate that same capability for a rookie in his first game. A machine could actually process even more than the experienced quarterback if it understands what to look for. For example, a defensive coordinator may consistently show an overload to one side on third and long but drops out of the play post-snap, blitzing from the alternate side in order to pressure a hot throw toward an eagerly awaiting defensive back. Armed with that information regarding what is likely to happen, the rookie quarterback could come to a better assessment and take an action with a higher probability of success.

We seek these same data-driven advantages as military leaders. Current technology holds the potential not only to replicate the knowledge and wisdom of a commander with three decades of experience but also to improve on this knowledge by processing beyond the limits of a single mind. This applies both to the tactical edge, where machine processing of data could shorten our kill chains and help us identify threats that current systems struggle to detect, and to the operational/strategic levels, where machine-enabled insights could help us understand adversaries' patterns of behavior to anticipate what they may do next and generate various response options.

That all sounds promising. But how do we make that concept a reality? Over the course of the last year, we at NC&N have undertaken a campaign to dramatically improve our critical capabilities to meet homeland defense requirements in an increasingly threatening security environment. This campaign has focused on speed and innovation, incorporating both internal efforts to experiment with commercial industry as well as with the Air Force as the operational lead for their first two JADC2 demonstrations. Through these initiatives, we have been putting the "J" in JADC2, rapidly advancing from concept to reality.

Our pursuit of this aim yielded a four-part concept that articulates the essential subcomponents that, when combined, constitute our vision of JADC2. This concept helps to move beyond the descriptive elements of JADC2 to actually explicate a framework to produce the capability. First, at its foundation, JADC2 is a data problem. It must draw on authoritative data sources, both historical and current, that are material to an understanding of the relevant security environment conditions. Second, that data must be cloud-based, accessible up, down, and across command echelons at the appropriate classification levels. Third, the data must be layered and ultimately fused across domains and reporting streams to enable operationally useful visualizations in an all-domain common operating picture (COP). Fourth, and most important, JADC2 must incorporate machine-enabled insights into that COP. These insights simultaneously leverage predictive analytics, machine and deep learning, and AI to better understand the situation and generate data-driven analyses that offer our leaders decision superiority. This concept is the framework we are using to make JADC2 a reality and overcome today's most pressing C2 challenges.

Figure 1. AI Analyzing Football Play in Real Time

C2 Today

The challenge that we have across the joint and allied forces is to operate at the speed of relevancy to deter and defeat today's threats. These threats have advanced to the point that they stress our ability to react swiftly enough to counter them. The challenges posed by modern weaponry, in both speed and stealth, place a premium on the time it takes to go from sensing a threat to directing an action by the best available shooter to defeat it. We may be able to identify a threat, and we may have defeat mechanisms in place to intercept it, but if we cannot process the information in time to execute, we are at an extreme disadvantage.

C2 today relies on myriad data sources that are collected and refined at each command level without a common interface. That data is stored in stovepiped silos with either proprietary or bureaucratic limitations that impose accessibility challenges. The result is different operating pictures at each level of command and across the seams between the commands, which hinders collaboration and reduces clarity. Beyond that, the decisions produced from this legacy architecture are subject to the limitations of human processing—idiosyncratic experience, knowledge, and the peculiarities of momentary happenstance.

We recently wrestled with the impact of these challenges when NC&N supported the Nation's COVID-19 response. As the outbreak spread, we received direction to lead DOD operations in the United States. Within 48 hours, we stood up both joint maritime and land component commands and established a flexible C2 architecture to support the dynamic employment of capabilities across the country, including the forward deployment of medical personnel into the heart of the outbreak in New York City. Using legacy C2 systems, we immediately found ourselves struggling to maintain situational awareness in order to inform the Nation's senior leaders as well as my own decisionmaking about what needed to be where and when to best accomplish our mission. In these early stages of the crisis, we used the traditional manual reporting through a hierarchical chain to aggregate data in Excel spreadsheets and PowerPoint slides, taking hundreds of hours to ultimately produce reports that were too stale to be useful.

Applying the JADC2 Concept

We were able to overcome the C2 challenges we faced at the outset of the COVID-19 response because of the unique opportunity it presented. There was a shared sense of urgency as part of the whole-of-nation effort, especially with commercial industry partners that were eager to assist. With them we were able to accelerate the progress on JADC2 development by applying the same four-part concept we had developed to address the homeland defense challenges posed by peer threats.

Solving the problem started with finding authoritative data, which meant moving data entry in most cases to the edge and cutting out redundant layers. For example, we accomplished this mission by working with two technology companies to deploy smart devices to forward-deployed units at places such as the Javits Center in New York City, where medical units could provide real-time status updates through custom-built apps and commercial online collaboration tools. This ability enabled us to track different statuses such as location, health, and personal protective equipment for these personnel. Moreover, the mobile

devices allowed me to virtually interact with the medical units to get the frontline pulse when I could not physically visit.

The second key step was to move that data to the cloud. We worked with the Joint Artificial Intelligence Center to host our data and enable industry entities to access it to produce operationally useful visualizations in the form of COPs. To accomplish this undertaking, we worked with two software companies to develop displays for not only medical statuses across the country but logistics and deployment information as well, providing real-time situational awareness across subordinate commands.

The pivotal part of our JADC2 concept, incorporating machine-enabled insights into the COP, proved most useful. We coordinated with an innovation laboratory and other tech firms to leverage predictive analytics to inform decisions. For example, we were able to bring in a number of data sources from across government and the private sector to develop a model that anticipated 2 weeks out where COVID-19 spikes were going to occur and where that outbreak would coincide with medical capacity shortfalls. Based on that model, I received a briefing on April 14 that identified a location of concern just north of New York City. Based on an exodus of people from Manhattan to the Connecticut suburbs, the model predicted an outbreak around Stamford, and we dispatched a surge of expeditionary medical capabilities in anticipation of the need for increased capacity. The model proved prescient. There were 412 new cases on April 19, and by April 22 that number had ballooned to 2,109.[1] Fortunately, we were able to get capabilities in place in time by drawing on the power of big data and predictive analytics to inform an operational decision. This success was largely due to a concerted and iterative effort to pursue JADC2 capabilities for homeland defense in the year leading up to the COVID-19 pandemic.

Delivering JADC2

Our COVID-19 response provided the opportunity for us to validate, leverage, and accelerate JADC2 initiatives that had begun the previous year as part of our homeland defense transformation. We had been well aware of our capability challenges at NC&N for quite some time and had conducted a series of studies over the years to understand our gaps and shortfalls as well as possible solutions to address advancing threats. In fact, there were so many different analytic efforts under way that we conducted a study of the studies just to understand how they all fit together. We learned that the myriad studies had reached a point of diminishing returns and that we needed simply to start solving the problem. We acknowledged that we would not get it exactly right out of the gate, but the newly adopted agile development approach allowed us to make iterative and rapid progress.

Based on that predilection for action, our JADC2 concept development took the form of praxis: taking the theory or idea behind JADC2—namely producing decision superiority—and actively attempting to build it out in the field. Knowing that time was not on our side, we employed an agile development model with technologically innovative commercial entities to break out of the standard capability procurement process. We thought big, started small, failed fast, and reinforced success. This approach included prototyping, experiments, and demonstrations over the last year aimed at producing the critical requirements needed to modernize our defenses.

The campaign started with a focus on shoring up potential vulnerabilities in air domain awareness to improve detection and responsiveness via a prototype called Pathfinder. Pathfinder harnessed the power of competition among industry innovators to quickly generate leap-ahead technology. Access to commercial industry was made possible through collaboration with the Defense Innovation Unit (DIU), bringing Silicon Valley talent to bear on our problem set. What DIU helped us create is a cloud-based data ecosystem that draws on disparate air domain feeds (for example, Federal Aviation Administration radars), pulling them into the cloud where data processors can run algorithms to identify tracks that legacy systems were unable to collect. This capability improves not only our sensing grid for identifying traditional offensive platforms such as aircraft but also the detection of launched weapons and unmanned aerial systems (UAS).

Pathfinder was only the beginning. We spearheaded additional experiments with commercial industry to improve detection against cruise missiles and UAS. We worked with companies that developed ML- and AI-enabled detect capabilities positioned at the tactical edge to identify a threat much earlier than previously possible, eliminating layers of reporting. In addition, these companies provided an advanced virtual user interface for the COP where the machine presented the operator with tasking options for various defeat mechanisms to intercept the missiles—in that case, a virtual engagement by an F-22 Raptor.

Based on the success of these early prototypes and experiments, the Air Force requested that we serve as the operational lead for the Advanced Battle Management System "onramp" number one. The Air Force and my team were focused on creating true JADC2 and had similarly adopted a DevOps approach in that pursuit.[2] Knowing the standard model to develop the needed capabilities would take too long, we were not afraid to try a different course. We cast a wide net, explaining our homeland defense needs to companies and agencies that could potentially be part of the solution. Rather than ask for specific capabilities, we described our challenges. When we found those with similar mindsets, whether in industry or across the Intelligence Community, we quickly merged our efforts to work toward mutually beneficial aims.

Because our team served as the vanguard for the onramp development, we were able to incorporate industry entities and government partners in prototyping and testing to quickly produce the results needed to illustrate what was within the realm of the possible. The first time we were able to successfully apply the JADC2 model with a wide range of joint

Connecticut National Guard Soldiers and Airmen set up 200 beds at Stamford Hospital and construct Alaskan Small Shelter System tents for separate triage area in response to COVID-19 pandemic (U.S. Air National Guard/Steven Tucker)

force participants happened at Eglin Air Force Base, Florida, in December 2019. The onramp scenario allowed us to collect authoritative data processed at the edge, pull those feeds into a data cloud, apply machine-enabled insights to present tactical-level employment options, and finally display that information in a multi-domain COP for the decisionmaker.

Through this pragmatic and iterative approach using experiments and demonstrations, we identified our process for building JADC2. A proven four-step concept emerged as a way to organize action and explain how one process leads to the next with the goal of achieving decision superiority: data—cloud—machines—COP.

Building JADC2

Authoritative Data. The first key to operating at the speed of relevancy is finding the authoritative data sources, prioritizing them, and removing redundant input layers. The effect of this operation

is the flattening of unnecessary layers within the C2 construct, thus removing potential for erroneous reporting and reducing hours of processing. Depending on the data in question, the authoritative source may be a sensor such as a radar feed, a traditional C2 node at a headquarters, or an open-source report coming through social media. When we think of our defenses for the homeland, we must look to identify and fuse feeds with all pertinent reporting streams to create a layered sensing grid from subsurface to on-orbit sensors that can support all-domain awareness from incoming threats.

Cloud Data Integration. That data must then be integrated into a cloud-based architecture that is openly accessible both vertically and horizontally across the echelons of commands and organizations that require its use. Importantly, that architecture must also be able to accommodate multiple classification levels, granting access based on the identity of the user to break down the

compartmentalized silos that exist today among organizations and partner nations that inhibit a unified and coordinated response.

All-Domain Common Operating Picture. Next, that data must be visually represented in operationally useful ways in the form of an all-domain COP. The feeds that are integrated into the visualizations must not only be layered but also fused to correlate tracks and reports to reduce uncertainty and increase assessment speed. Ideally, the COP would have multifunctionality, with the ability to toggle among a variety of customizable visualizations within one framework rather than relying on multiple COPs that necessitate greater manning and human-to-human processing. Instead of a static output, user-defined visualization permits operators to select the data sources that they are concerned with as well as to tailor the manner of display to best enable understanding and decisionmaking. In the digital age, data-rich machine-based analytics demand
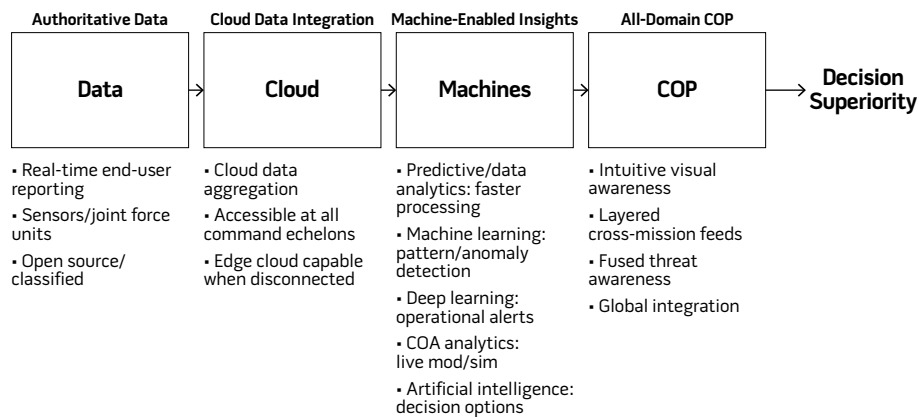
sophisticated user-friendly visualization to optimize decisionmaking. Our current prototype COP operates in just this way; it is data- rather than platform-based, applying technology to meet the emerging needs of a commander. The production of a COP that provides a rich understanding of the current situation and how it came about is the termination point of most C2-enhancement efforts before now. While those aims certainly advance beyond where many commands are today, it does not enable decision superiority on par with what we need to contend with the threats of today as well as tomorrow. To ensure superiority, we must employ tools that allow us to anticipate what will likely happen in the future and assess our options. This is where machines are required. Advanced processing power, ML, and AI can take C2 to another level (see figure 2).

Machine-Enabled Insights. Machines are *the* key component of JADC2. They offer the potential to move beyond our human limitations and create a better understanding not only of the current situation but also of the future—and how our potential actions are likely to play out. We have long had goals to produce this type of technological foresight capability. The difference is the capabilities to produce this insight are no longer the substance of science fiction. They are readily employed across virtually every aspect of our lives, from car navigation to tailoring online shopping options. The power of machines needs to be unleashed not only to enhance our way of life but also to protect our lives themselves.

To accomplish this goal we must call on machines to perform a variety of functions in support of JADC2. First, employing big data and predictive analytics could allow us to process large amounts of information that would otherwise take thousands of human hours. This ability speeds up processing and creates a deeper appreciation of the situation at hand. Today it takes legions of analysts poring over reams of intelligence data to establish connections between their observations. If the subject of their inquiry could be translated into a task for a machine to process, exponentially more data could be analyzed and many more

Figure 2. USNORTHCOMJADC2 Concept

Authoritative Data	Cloud Data Integration	Machine-Enabled Insights	All-Domain COP	
Data	**Cloud**	**Machines**	**COP**	**Decision Superiority**

- Real-time end-user reporting
- Sensors/joint force units
- Open source/classified

- Cloud data aggregation
- Accessible at all command echelons
- Edge cloud capable when disconnected

- Predictive/data analytics: faster processing
- Machine learning: pattern/anomaly detection
- Deep learning: operational alerts
- COA analytics: live mod/sim
- Artificial intelligence: decision options

- Intuitive visual awareness
- Layered cross-mission feeds
- Fused threat awareness
- Global integration

meaningful connections might be identified, freeing up analysts to focus on tasks that only a person is able to tackle.

Next, we could look to ML to incorporate historical data and identify significant patterns and anomalies that might indicate an adversary's intent. For instance, we might learn over time that certain indicators are correlated with military maneuvers beyond those that we might typically associate. Commodity prices near a base could fluctuate. Ordering for replacement parts for military equipment could precede deployments in predictable patterns. All these could serve as queues to help us better anticipate when something anomalous or consistent with a concerning activity is occurring.

Beyond that, machines could link those ML-enabled detections together to produce deep learning. Deep learning would help us establish a broader pattern of life for the adversary that could generate operational alerts when there is a confluence of concerning indicators. Those processes incorporate real-time and historical feeds to create an understanding of what has happened, is happening, and is likely to happen. By allowing machine and deep learning to identify whole new subsets of observable behaviors or conditions, we potentially move our decision space to the left of launch, giving us greater flexibility and more time to prepare a response.

We could also leverage machines to incorporate the hypothetical. By layering modeling and simulations for both

enemy and friendly actions into the same interface, we could allow the machine to run multiple scenarios against various contingency force postures. Employing AI against these simulations affords the machine the opportunity to iteratively learn and develop options for decision. The options generated through this data-rich process place the decisionmaker in an advantageous position by providing recommendations, implications, and follow-on effects along with concomitant risks.

This is made possible by increasing both the breadth and depth of the data analysis. We are not just talking about having a computer generate some prescribed responses based on a few indicators. Increasing the breadth of the data pool provides the opportunity to expose novel correlations that we could link to adversary behavior. The depth of the analysis afforded by advanced analytics allows for a much richer understanding of a situation over time by incorporating orders of magnitude more data than we currently use. For example, Monte Carlo analysis could provide much deeper insight into a wide range of possible future outcomes and the risks associated with them.[3] This data-driven approach provides highly granular understanding to move decisionmaking from reactive to anticipatory and proactive. Decisionmakers could have more sophisticated insight into complex problems and make decisions with much clearer understanding of the ramifications on future operations.

General Terrence O'Shaughnessy addresses National Defense University's combined colleges as part of University's President's Lecture Series, at Fort Lesley J. McNair, Washington, DC, April 21, 2019 (NDU/Katie Persons Lewis)

To be clear, humans will still make the decision, but they will do so from a much more informed perspective based on the input from machines. Today, when a crisis situation arises, I rely on a colonel with over 20 years of experience and his or her team on the watch floor of our USNORTHCOM and NORAD Command Center to help me make decisions. This team rapidly processes the information that is projected onto a bank of screens from a vast number of reporting feeds. These individuals, each responsible for a different aspect of the complete picture, correlate and make sense of that data as quickly as possible using only their innate processing power, doing an admirable job given their current capability suites. However, the technology exists today for us to do much better. Only by fully harnessing the potential of machines will we ultimately achieve JADC2's goal of producing decision superiority.

Today's security environment requires military leaders to be armed not just with current information, but also with operational insights that will enable better and faster decisions. Keenly aware of this immediate need, we at USNORTHCOM and NORAD have led the charge working with both DOD and commercial industry partners through an iterative approach to build that capability. Our efforts to jump from the PowerPoint slide to the field yielded a four-part concept that disambiguates JADC2 and accomplishes two important things: first, it provides a framework that makes it easier to orchestrate efforts to create and enhance JADC2 for our formations; second, it helps articulate how JADC2 differs from previous C2 advancement initiatives—namely the inclusion of machine-enabled insights to identify anomalous events, predict what is likely to happen next, and generate options that overcome human limitations. This is a significant progression from where we were on this effort just a few years ago, but we cannot rest. We must continue this unrelenting pursuit for JADC2, as it is the core capability that the joint force needs to fight and win in the digital age. Because of the work we have done with innovative teams in an agile development model, we now have a better understanding of what we need JADC2 to do and how to make it real. Decision superiority, enabled by JADC2, is the competitive advantage we need against peer adversaries. **JFQ**

Notes

[1] Patrick Tucker, "How the Pandemic Is Helping the Military Prep for World War III," *Defense One*, May 26, 2020, available at <www.defenseone.com/technology/2020/05/how-pandemic-helping-military-prep-world-war-iii/165656/>.

[2] DevOps refers to an approach that combines software development with operations to increase the rate of innovation.

[3] Monte Carlo analysis is a method that uses statistical evaluation of randomized data sets to better understand things such as probability distribution.

Chaplain (Captain) James Johnson, USN, presents gift to Supreme Patriarch of Thailand during exercise Cobra Gold, in Bangkok, Thailand, February 12, 2018 (U.S. Navy/Ian Kinkead)

Rightsizing Our Understanding of Religion

By Wayne A. Macrae

Chaplain (Captain) Wayne A. Macrae, USN, is Chaplain to the Chairman of the Joint Chiefs of Staff.

The world of religion consists of various belief systems that influence humanity in numerous ways. Religion is global. It is powerfully influential everywhere that the joint force currently operates and extends to every corner of the globe. Religion is part of the fabric of every nation—including those that take a position against it. For governments that identify as secular or atheist, religion remains a present factor that they work to account for or control both internally and externally. Every government invests time and energy in controlling, influencing, or seeking to exist alongside religion.

In recent years, religious boundaries have begun to shift as immigration has surged, creating more overlap, interaction, friction, conflict, and competing interests of diverse influences. Understanding the interchange among intersecting religious dynamics, strategic theater goals, plans, and military operations is at the heart of global integration; this is particularly true when considering the presence of religion throughout the "gray zone" between peace and war and the major role of religious dialogue in messaging to and influencing adherents. This article advocates for a strategic approach to religion and the role of the

chaplain in representing it to the commander. The article also considers the dynamics and growing impact of religion, how nations interact with it, U.S. military interaction with religion, and how the U.S. military could account for that role through the utilization of religious affairs staff sections.

The world's main religions have been present for thousands of years—a feat no government present today can boast. Philosophies and ideologies likewise come and go, though they may leave their mark on religion for a time. Religion has influenced cultures throughout history, and, frankly, it would be a denial of history to expect the influence of religion to cease in the future. History attests to the great resilience of religion and to the role it plays in regional trends and geopolitics.

Religion is a key influencer in the cultures and practices of many allies, unified action partners, and enemies. While Western European and North American culture may regard religion as being personal and private, most regions of South America, Africa, the Middle East, and Asia view religion and religious figures as key influencers within society, with the topic of religion itself regarded as corporal and public. For the vast majority of people, religion and religious faith informs not only how they view their world but also how they live their daily lives and respond to the institutions around them.

The Western cultural bias toward the place of religion creates a blind spot that causes many in the West to minimize the role and importance of religion in other societies. As Chaplain Paul Wrigley, Naval Academy graduate and former naval aviator, stated:

An operational commander, however well trained in the military issues, who is ignorant of or discounts the importance of religious belief, can strengthen his enemy, offend his allies, alienate his own forces, and antagonize public opinion. Religious belief is a factor he must consider in evaluating the enemy's intentions and capabilities, the state of his own forces, his relationship with allies, and his courses of action.[1]

The Growing Impact of Religion

Research paints the picture of a steadily increasing global majority holding to a religious faith and identification. According to a Pew Research report, population trends indicate a continued increase in faith among the major religions, while nonreligious populations continue to decline. Current estimates are that 84 percent of the global population follows a religious faith; by 2050, 87 percent of the global population could adhere to religious faith.[2] According to the same report, much of this growth is projected to take place within the following regions:

- Asia-Pacific, with 21.8 percent projected growth in major religious groups
- Latin America and the Caribbean, with 26.9 percent projected growth
- Middle East and North Africa, with 72.7 percent projected growth
- Sub-Saharan Africa, with 130.9 percent projected growth.[3]

These regions correspond to U.S. Indo-Pacific Command, U.S. Southern Command, U.S. Central Command, and U.S. Africa Command, respectively. These four commands are geographic combatant commands (CCMDs) that provide command and control of military forces in peace and war.

Strategic Approaches to Religion
As noted in the 2017 National Security Strategy, the United States views the freedom of religion as a fundamental individual liberty and remains committed to supporting and advancing religious freedom.[4] This is a foundational principle of our Republic and acknowledges a key reality of governmental dynamics. All governments develop approaches for dealing with religion or religions. There may be one principle—such as the U.S. stance on religious freedom—or there may be several approaches, depending on which religion is the focus of attention. The relationship between governments and religions are often dynamic and changing. When we consider the challenges identified in our National Defense Strategy, we cannot help but note that those groups who pose external threats

exhibit efforts to oppose or control religion and religious expression.[5]

Russia uses religion, as expressed through the Russian Orthodox Church (ROC), as an instrument of national soft power. Russian Federation President Vladimir Putin positions himself as the protector of Christian Orthodoxy cast against a secular West that has lost all moral sensitivity and direction. According to Jack Dulgarian:

The Kremlin has given the ROC the spotlight in its state-sponsored media, stressing the importance of Orthodox Christianity to contemporary Russian life. It is closely related to Putin's effort to portray himself as a vanguard of traditional, conservative values. On major Christian feast days, Putin and prominent Russian politicians are regularly shown lighting candles inside grandiose cathedrals, as well as in small village churches—serving to cement the image of church-state unity.[6]

It also is Russia's practice to construct Orthodox churches among Russian minority populations as centers for unity, identity, and influence—and as potentially destabilizing outposts in nations bordering Russia.

China is politically atheistic and seeks to control or limit religion. Open-media sources report significant crackdowns on various religious groups, particularly the Muslim Uighur population in the western province of Xinjiang. The Chinese government strives to be in control of religion. As Thomas Harvey notes:

In the history of the People's Republic of China, President Xi Jinping is the first paramount leader to give prominence to religion in word and deed. In a major speech in 2016, Xi called for the "sinicization of religion."

He noted that, given the rise of religion among the Chinese people, the Chinese Communist Party (CCP) must "guide the adaptation of religions to socialist society." In its academic sense, "sinicization of religion" refers to the indigenization of religious faith, practice, and ritual in Chinese culture and society. For Xi,

Lieutenant Colonel Lucilio Mizerani, USA, 18th Medical Command (Deployment Support) chaplain, administers religious support to fellow team members in Yona, Guam, April 18, 2020 (U.S. Army/Luisito Brooks)

however, "sinicization" is profoundly political. It requires religious leaders and institutions demonstrably to embrace State Socialism and the leadership of the CCP.[7]

The Council on Foreign Relations reports the widespread growth of religion among the Chinese population; by some estimates, China may have the largest Christian population in the world by 2030.[8] Religious attitudes and national policy will increasingly conflict, as the 6 percent of the Chinese population who make up the CCP become more out of step with the growing religious population. Additionally, China's Belt and Road Initiative puts the country in contact with strongly religious populations across Eurasia. To advance its national agenda, China will need to adjust its approach to religious populations and gain a better understanding of the untapped soft power of religion.

Iran is a theocratic state that uses religion to control its population. According to Greg Bruno:

Under Khomeini, the Iranian religious and political landscapes were dramatically transformed, making Shia Islam an inseparable element of the country's political structure. Khomeini ushered in a new form of government anchored by the concept of velayat-e faqih, or rule of the Islamic jurist. In his 1970 book, Hokumat-e Islami: Velayat-e faqih, Khomeini argued that government should be run in accordance to sharia, or Islamic law. For that to happen, an Islamic jurist—or faqih—must oversee the country's political structure.[9]

Religion is a primary ideological factor in Iran's foreign policy, which is overseen by the supreme leader—a cleric. Iran's constitution grants the supreme leader's office almost unlimited power.

According to Haidar Kherzi, "Today, Khamenei—like his well-known predecessor Ayatollah Khomeini, whose reign ended when he died in 1989—wields enormous control over Iran's military, judiciary, treasury, media, foreign policy, presidential cabinet, and legislative process."[10]

North Korea maintains a strong atheism, blocking or manipulating religious expression while simultaneously establishing a form of "emperor worship," in the philosophy of *juche*, to control the population. According to Grace Lee:

When Kim Il Sung unilaterally declared juche to be the governing principle of all aspects of North Korean life, as well as the ideological basis of all state policies, the philosophy gained the full authority of Kim Il Sung's godlike status. Having established the infallibility of the juche philosophy and consolidated their own political power,

KFOR Regional Command–East Liaison Monitoring Team K18, comprising Soldiers from 2nd Battalion, 162nd Infantry Regiment, Oregon National Guard, RC-E Chaplain (Captain) Katie Declet, and Religious Support Specialist (Specialist) Darren Anderson from 2nd Battalion, 135th Aviation, Colorado National Guard, meet with Father Srdjan at historic Church of Sveti Nikola in Kamenica, Kosovo, on August 3, 2020 (U.S. Army National Guard/W. Chris Clyne)

Kim Il Sung and Kim Jong Il were able to use juche principles of self-sustenance and political and military independence as justification for policies such as the routing of a huge percentage of national income toward military expenditures, despite the famine sweeping through the populace. Due to the power and influence of one man, the Great Leader, the juche philosophy became inextricably embedded in the economic, political, military and cultural aspects of life in [North Korea].[11]

There are also reports of growing clandestine religious organizations in North Korea that can further challenge the regime's efforts to oppress religious expression.[12]

Violent extremist organizations such as the so-called Islamic State (IS) and al Qaeda perversely claim to find justification in the Quran for their atrocities. As reported in the *New York Times*, IS "leadership has emphasized a narrow and selective reading of the Quran and other religious rulings to not only justify violence, but also to elevate and celebrate each sexual assault as spiritually beneficial, even virtuous."[13]

Beyond authoritarian regimes, all nations invest time and energy dealing with the realities of religion within their borders. One way of gauging a nation's response to religion is to plot that country's stance on religious freedom issues. An example is the Department of State's Annual Report to Congress on International Religious Freedom, which describes the status of religious freedom across countries; government policies violating religious belief and practices of various religious groups; and U.S. policies promoting religious freedom. The lesson from this information is that the impact of religion on governments and policies is diverse. Because simple assumptions will often be inaccurate, the U.S. military must consider the multitude of distinctions for how a nation's relationship with religion can and will influence our military interactions. When the U.S. military acts in conjunction with partner nations—either bilaterally or in coalitions—the religious landscape

becomes even more dynamic. The mix of thoughts, attitudes, and convictions regarding religions becomes quite forceful. Consequently, the joint force requires a robust understanding of religion, religious issues, internal and external factors influencing religion, and, ultimately, regional stability.

The U.S. Military and Religion
The relationship between the U.S. military and religion goes back to the beginning of the Nation. According to the Army History Center, the "Chaplain Corps dates back to 29 July 1775, when the Continental Congress authorized one chaplain for each regiment of the Continental Army, with pay equaling that of a captain."[14] Not long after, the Navy Chaplain Corps was formed. According to Douglas Stutz, the

Chaplain Corps traces its beginnings to 28 November 1775 when the second article of Navy Regulations was adopted. It stated that "the Commanders of the ships of the thirteen United Colonies are to take care that divine services be performed twice a day on board and a sermon preached on Sundays, unless bad weather or other extraordinary accidents prevent."[15]

For more than half of its history from 1775, the Chaplain Corps' almost sole focus has been the provision of religious support for the direct spiritual needs of our military personnel.

But that situation began to change with the Cold War. As noted in a Joint Staff History Office information paper, the changing character of that conflict saw chaplains "tasked to go beyond their primary mission of pastoral care and provide advice on the effect of religion on military operations."[16]

Subsequent conflicts in Vietnam, the Balkans, Iraq, and Afghanistan have increasingly drawn the chaplaincy into an advisory role, with chaplains, consistent with their noncombatant status, counseling on the impact of religion for military operations. Joint Publication 1, *Doctrine for the Armed Forces of the United States*, identifies religious advisement as addressing "the commander's requirement to

receive germane subject matter advice on the impact of religion on operations. All military commanders are responsible for religious affairs in their command."[17] In addition, chaplains were brought into dialogue with religious leaders, both civilian and military, in pursuing the amelioration "of suffering, the promotion of peace, and the benevolent expression of religion."[18] The net effect is that military chaplains have been providing religious advisement to commanders for over 70 years.

It is important to make a significant distinction here: These examples are set against the backdrop of phases of war. Today, the nature of operations is more fluid. As JP 3-0, *Joint Operations*, states, the "complex nature of the strategic environment may require U.S. forces to conduct different types of joint operations and activities simultaneously across the conflict continuum."[19] As the nature of operations continues to change and the continuum develops further into areas of competition, the ability to understand and account for the impact of religion will grow in importance.

One of the major efforts from the National Defense Strategy is that of strengthening alliances and attracting new partners.[20] In a world where religion plays a major role, and with religious freedom as a key principle within the National Security Strategy, the ability to demonstrate our appreciation for religion and religious freedom through willful engagement with religions and religious actors will speak volumes about the sincerity of our claims and intentions.

Despite the religious plurality and diversity within the United States, there is an amazing degree of unity and cohesion. Our military embodies this harmony within the Chaplain Corps. Our military's engagement with religion models for other nations how to build cooperation— rather than friction— when it comes to religion.

Religious Advisement as Strategic Enabler
At this point, we could justifiably ask what the problem is if the military has taken advantage of religious advisement for over 70 years. The problem is that

religious advisement as an enabler, and the benefits it brings for military operations, is not completely understood or applied. Although commanders do embrace the religious support role of chaplaincy to take care of the religious needs of U.S. military personnel, the recognition of religious advisement as an enabling function with utility to the commander is spotty at best—primarily limited to ground commanders who have previously benefited from the practice of religious advisement. Couple this situation with the Western bias against religion, and we find ourselves needing to relearn the same lessons. The answer is to institutionalize—across the joint force—the understanding of religious advisement as a necessary enabler.

It's clear just from looking at policy and staffing that the entire joint force does not regard religious advisement as a key enabler. The Army has extensive guidance on religious support and external advisement contained in Army Techniques Publication 1-05.3, *Religious Support and External Advisement*, which provides 60 pages of material and dates from January 2019.[21] The Navy's guidance on *Chaplain Advisement and Liaison*, Secretary of the Navy Instruction 1730.10A, covers five pages on external religious advisement.[22] Finally, Air Force Instruction 52-101, *Chaplain Planning and Organizing*, provides one page of material covering religious advisement.[23] The amount of effort and attention that the three Services devote to religious advisement policy and doctrine drives the level of understanding and interest within each Service and has a corresponding impact on CCMDs.

Staffing levels for chaplain billets across CCMDs likewise communicate a great deal regarding the overall expectations placed on those offices. CCMD chaplain teams range from zero billets at one command to a high of four billets at another. If the goal is to provide religious support only for assigned staff, these numbers may be adequate. However, if an appreciation truly existed for religious advisement as a staff function and force enabler at work across the staff and cross-functional teams, then it is hard to

conceive of two or three individuals accomplishing the advisement and religious support task within a command.

What Should Religious Advisement at the Strategic Level Look Like?

It is one thing to make a claim that chaplain support to a CCMD should be organized into something more than a one- or two-person team; it is another thing to justify that expansion. So, what would be the benefit for a CCMD if it bought into the idea of creating a religious affairs staff section?

First, the combatant commanders could expect to gain a deeper appreciation for the religious dynamics within each country in their areas of operation. A religious affairs section could work with interagency offices that focus on religious issues and the extensive network of religious affairs teams across Service components. It could build expertise and understanding at the strategic level of not only major religions but also the primary issues, key personalities, and major influencers within each religious movement and geographic region. With central coordination at the CCMD level, products generated at component levels, such as religious area analysis and port call reports, could be rolled up, collated, and shared for analysis and increased understanding, rather than stovepiped and isolated. Collating such information would also identify which areas demand additional analysis and where dynamics are shifting over time. This in and of itself is no simple task: It requires dedicated work hours to build and manage. But the potential benefit to military operations would be invaluable, and the effort would strengthen our relations with allies and partners.

Second, a functional religious affairs staff section would enable coordination among the Service components and National Guard units participating in the State Partnership Program (SPP). This program links a state's National Guard, as a unique component of the Department of Defense, with the armed forces of a particular country in a cooperative relationship.[24] Currently there are 78 partnerships in effect involving all 54 States and Territories. As Chaplain (Lieutenant Colonel) Kurt Mueller points out, "the SPP is a low cost, high payoff program that is ready for further development in the area of religious diplomacy."[25] Such coordination would minimize duplication of effort in support of partner-nation chaplaincies, identify gaps in support to partner-nation chaplaincies, and ensure that efforts among partner nations are synchronized with the commander's overall priorities within the area of operations. This effort would also ensure that CCMD staffs remain aware of the religious engagement efforts already in place within the geographic area and that the commander's priorities are reflected in component and State Partnership Program engagement strategies.

Third, when Embassies need to engage with religious actors within an assigned country, a sufficient religious affairs staff would be able to assess requests for religious leader support/engagement and work with the various components and National Guard units to offer the best support the Embassy requests, in conjunction with CCMD direction and guidance.

Finally, a sufficiently staffed and resourced religious affairs section could coordinate among various staff codes, working groups, cross-functional teams, and so forth. This ability, in turn, would ensure that the role of religion is adequately represented in problem analysis and courses of action development, plans development, command messaging, and engagement strategies. A properly staffed religious affairs section could do all these things to further the command's mission within the geographic area—while still being able to carry out the core function of providing direct religious support to and general care for the staff.

Recommendations

It is worth noting again that some of the elements discussed here are already found within pockets of the military; the challenge is that the role of religious affairs is not universally understood or experienced. Over the past few decades, many writers have called for an increased role for religious engagement, noted the growing impact of religion on military operations, and pointed to examples in which religious leader engagement has had positive impacts.[26] To ensure that the acceptance of religious advisement as enabler for the commander gains traction, more needs to be done than just raising awareness. This concept must be integrated into existing strategic-level military education.

Our leaders at the general and flag officer ranks will benefit from understanding that religion is something more than just a resource used to support their personnel. Professional military education should expose general and flag officers to the multifaceted nature of all religions as well as the complex ways in which governments choose to interact with religions and religious expression. This will result in a deeper appreciation for the influential role religion still plays in societal identity, perception, and national will.

Furthermore, the Service chaplaincies need to focus on preparing chaplains to serve in the joint environment and at CCMDs; this means preparing chaplains to understand the larger issues involved in external religious advisement, understanding the dynamics of religious developments, and gaining practice in the principles of religious leader engagement. The Service chaplaincies should strengthen their preparation of chaplains to serve in the joint force and highlight joint policy through their intermediate and advanced officer training courses. Services should also ensure that chaplains who receive funded graduate education in world religions or religion and culture courses serve in assignments that allow them to contribute to the knowledge pool required to support components and CCMDs.

Finally, the Department of Defense should consider the benefit of—and invest billets and resources in—establishing religious affairs sections with the bandwidth to provide both religious advisement and religious support to senior-level staffs. Those commanders who receive both counsel and support will be properly positioned to understand

and interact with the persistent and prominent role of religion in the global arena. **JFQ**

Notes

[1] Paul R. Wrigley, "The Impact of Religious Belief in the Theater of Operations," *Naval War College Review* 49, no. 2 (Spring 1996), 84–101, available at <https://www.jstor.org/stable/44642870>.

[2] Pew Research Center, *The Future of World Religions: Population Growth Projections, 2010–2050* (Washington, DC: Pew-Templeton Global Religious Futures Project, 2015).

[3] Ibid., chapter 3.

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

[5] *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).

[6] Jack Dulgarian, "The Most Important Thing to Understand About Putin's Russia," *Merion West*, October 14, 2019, available at <https://merionwest.com/2019/10/14/the-most-important-thing-to-understand-about-putins-russia/>.

[7] Thomas Harvey, "The Sinicization of Religion in China—Will Enforcing Conformity Work? *Evangelical Focus*, September 30, 2019, available at <https://evangelicalfocus.com/lausanne-movement/4780/the-sinicization-of-religion-in-china-will-enforcing-conformity-work>.

[8] Eleanor Albert, "Christianity in China," *Council on Foreign Relations*, October 11, 2018, available at <https://www.cfr.org/backgrounder/christianity-china>.

[9] Greg Bruno, "Backgrounder: Religion and Politics in Iran, *New York Times*, June 19, 2008, available at <https://archive.nytimes.com/www.nytimes.com/cfr/world/slot3_20080619.html?_r=1&pagewanted=print>.

[10] Haidar Khezri, "Unrest in Iran Will Continue Until Religious Rule Ends," *The Conversation*, January 23, 2018, available at <https://theconversation.com/unrest-in-iran-will-continue-until-religious-rule-ends-90352>.

[11] Grace Lee, "The Political Philosophy of Juche," *Stanford Journal of East Asian Affairs* 3, no. 1 (Spring 2003), 105–112.

[12] Nazanin Zadeh-Cummings, "True Believers: Faith-Based NGO in North Korea," *NK News*, March 14, 2017, available at <https://www.nknews.org/2017/03/true-believers-faith-based-ngos-in-north-korea/>.

[13] Rukmini Callimachi, "ISIS Enshrines a Theology of Rape," *New York Times*, August 13, 2015, available at <www.nytimes.com/2015/08/14/world/middleeast/isis-enshrines-a-theology-of-rape.html>.

[14] Army History Center, "U.S Army Chaplain Corps," n.d., available at <https://armyhistory.org/u-s-army-chaplain-corps/>.

[15] Douglas H. Stutz, "Happy 239th—Chaplains Corps Birthday Held at Naval Hospital Bremerton," *Navy.mil*, November 27, 2014, available at <https://www.navy.mil/submit/display.asp?story_id=84667>.

[16] Christopher Holmes, "History of Chaplains and Advising on Religious Affairs," information paper, Joint History Office, April 4, 2019.

[17] Joint Publication JP-1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, Incorporating Change 1, July 12, 2017), IV-22.

[18] Joint Guide 1-05, *Religious Affairs in Joint Operations* (Washington, DC: The Joint Staff, February 1, 2018), III-6.

[19] Joint Publication JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017, Incorporating Change 1, October 22, 2018), V-4.

[20] *Summary of the 2018 National Defense Strategy of the United States of America*.

[21] Army Techniques Publication 1-05.3, *Religious Support and External Advisement* (Washington, DC: Headquarters Department of the Army, January 2019).

[22] Secretary of the Navy Instruction 1730.10A, *Chaplain Advisement and Liaison*, August 28, 2018.

[23] Air Force Instruction 52-101, *Chaplain Planning and Organizing* (Washington, DC: Headquarters Department of the Air Force, July 15, 2019).

[24] National Guard, "State Partnership Program," n.d., available at <https://www.nationalguard.mil/Leadership/Joint-Staff/J-5/International-Affairs-Division/State-Partnership-Program/>.

[25] Kurt Mueller, "Religious Diplomacy: Exporting Military Chaplain Professionalism," *The U.S. Army Chaplain Corps Journal*, CY2018 edition, available at <https://ufdcimages.uflib.ufl.edu/AA/00/06/88/10/00001/2018.pdf>.

[26] William Sean Lee, Christopher J. Burke, and Zonna M. Crayne, *Military Chaplaincies as Peace Builders: Embracing Indigenous Religions in Stability Operations*, The Cadre Papers 20 (Maxwell Air Force Base, AL: Air University Press, February 1, 2005); Bradford E. Ableson, "A Time for Conversion: Chaplains and Unified Commanders," *Joint Force Quarterly* 32 (Autumn 2002), 98–103; Eric Patterson, ed., *Military Chaplains in Afghanistan, Iraq, and Beyond* (Lanham, MD: Rowman & Littlefield, 2014).

Paratroopers assigned to 173rd Airborne Brigade conduct inspections prior to airborne operations in Grafenwoehr Training Area, Germany, July 23, 2020 (U.S. Army/Ryan Lucas)

Success on Purpose
A Message for Leaders of Military Organizations

By Russell Steven Williford and Wendi Peck

Colonel Russell Steven Williford, USAF, is the Vice Wing Commander of the 341st Missile Wing, Malmstrom Air Force Base, Montana. Wendi Peck is the CEO of Executive Leadership Group, Inc.

W hy do leaders of successful military operations often struggle to recreate that success when placed in charge of standing military organizations? What do the leaders of highly effective military organizations have that is missing for organizational leaders struggling with cultures mired in bureaucracy and box-checking?

We propose that highly successful military operations and organizations share a feature that is so obvious it is easy to miss: Their teams have been given a clear *and* meaningful purpose—an elevating "why" behind their work—that they understand and embrace. This phenomenon appears to occur more naturally with active military operations than with standing military organizations. But when it does occur, the result is a committed unit that is outcome-focused and agile, prioritizes smartly, and innovates or adapts as needed. Clear and meaningful purpose also begets collaboration; people with a common purpose tend to work well as a team, even if they have little else in common.[1] These teams attract and retain top-tier talent. The ultimate outcome is success—success on purpose—whether in a relatively short operation or in a long-standing organization.

Thus, the aim of this article is threefold. First, we intend to establish communication of clear and meaningful purpose as more than just a nice-to-have skill for military leaders. In fact, a wealth of research has spelled out both the criticality and the characteristics of team members' connections to their team's particular purpose. Second, based on our own research and experience within the Department

---

of Defense, we argue that active military operations and standing military organizations have vastly different levels of purpose-driven leadership. Leaders of operations tend to guide their teams with clear and meaningful purpose; leaders of organizations tend to struggle to elucidate the organization's purpose and connect it to every member. Finally, we review four ways by which effective leaders connect their teams to purpose. We attempt to offer that information with sufficient range and specificity so leaders at all skill levels will find actionable information to help them achieve their unit's purpose.

More Than a Nice-to-Have: A Requisite for Success

When a team has a purpose that its members find both clear and meaningful, that purpose drives the team toward success. Both those aspects of purpose—clarity and meaningfulness—have been studied exhaustively in military and nonmilitary settings. Here, we emphasize the importance of both.

Clarity. Aristotle distinguished between *telos*, the result or purpose of something, and *techné*, the means of achieving a purpose. It is a useful distinction. Purpose answers the question, "What are we trying to achieve?" That often is harder to answer than, "What are we doing?" For any military team—from fully operational to fully supporting—purpose must answer the question, "Why does our unit exist?" or, at a minimum, "What outcome or accomplishment are we aiming for?" The answer must be specific enough that members know when their unit's purpose has—or has not—been achieved. In other words, core mission outcomes must be verifiable.

When a team understands the unit's purpose in terms of verifiable outcomes, it has the unifying focus that is foundational for successful performance, including the informed decisionmaking required for innovating or adapting to achieve success. In their examination of 75 work teams, researchers Carl Larson and Frank LaFasto found that, "without exception, when an effectively functioning team was identified, it was described by [its members] as having a clear understanding of its objective."[2] All the poorest performing teams were missing this clarity.

Meaningfulness. Yet knowing a team's purpose, even if it is clear, does not suffice to drive team members toward accomplishing that purpose. Something else is needed. Austrian psychiatrist Viktor Frankl is best known for his work advocating for the importance of meaning. A Holocaust survivor, Frankl theorized that those interned in the concentration camps who had a higher purpose were more likely to survive, and in his writings he encouraged finding meaning by embracing activities that connect the individual to something greater. He often quoted Friedrich Nietzsche: "He who has a 'why' to live can bear almost any how."[3]

Today, many people want to find meaning in the higher purpose they serve through work. Decades of research have shown that meaningfulness often outweighs other occupational features, including job security, income, and career advancement opportunities.[4] This is good news at a time when the military is struggling to attract and retain talent.

In his book *Drive: The Surprising Truth About What Motivates Us*, Daniel Pink devotes an entire chapter to purpose, where he writes, "The most deeply motivated people—not to mention those who are most productive and satisfied—hitch their desires to a cause larger than themselves."[5] Research supports Pink's assertion, but with provisos: There are aspects of purpose, aside from clarity, that make it meaningful. We cite four that all leaders should know.

First, and perhaps most obvious, a unit's purpose must be perceived by team members as meaningful. This requires a leader to help team members elevate their focus from the actions that must be performed to the important and positive outcomes that should result.[6] For example, an Air Force maintenance group commander explained his success by stating, "It is about helping our maintainers see that it's not just a collection of tasks that we do. It's about the combat capability we produce on a daily basis that is used to shape world events."

Sometimes the meaningfulness of a purpose stems from how that purpose is described. Consider the following two descriptions of one defense organization's purpose: The Defense Prisoner of War/ Missing in Action Accounting Agency Web site states that its mission is to "[p] rovide the fullest possible accounting for our missing personnel to their families and the nation."[7] That is a good and noble purpose. But we recently heard another description of that same purpose that might convey a more powerful meaning to the agency's team.

Dr. Kyle McCormick, a forensic anthropologist with the agency, stayed late to show two strangers—one of the authors and her 13-year-old granddaughter—what the agency does. That evening, among gurneys holding warfighters' remains, he answered the question, "Why do you think this agency exists?" His answer was immediate, and it reflected the meaningfulness of the mission: "We keep America's promise to bring everyone home."

Second, meaningfulness comes from a personal connection. Team members who understand both their unit's higher purpose *and* their own contribution to it are more likely to see their work as meaningful. Recall the story of the National Aeronautics and Space Administration (NASA) janitor who stated, "I'm not mopping the floors, I'm putting a man on the moon."[8] That attitude did not happen by accident. A recent study of NASA's Manned Lunar Landing Program revealed a key component of its success. People were not simply told NASA's larger purpose. Rather, they were shown exactly how they and their work fit into it. It was a deliberate, orchestrated organizational strategy for success. Later, we describe how individual leaders can do the same.

Third, critical to meaningfulness is that the unit's purpose be seen as "difficult but achievable."[9] Challenge—especially one unique to the unit or unit type—increases the meaningfulness of the unit's purpose. Of course, the goal must be more than just theoretically achievable; team members must see it as achievable by *them*. Members' belief

Soldiers from 3rd U.S. Infantry Regiment and Chaplain (Lieutenant Colonel) Sid Taylor, USA, help conduct funeral honors with escort for U.S. Army Air Forces Captain Lawrence Dickson, MIA since December 1944 after plane crash in Austria, in Section 60 of Arlington National Cemetery, March 22, 2019 (U.S. Army/Elizabeth Fraser)

that their team has the skills, tools, and resources to meet the challenges ahead is strongly related to high performance.

Fourth, meaningfulness requires a level of autonomy. When unit members are empowered with appropriate autonomy, their ownership of the unit's purpose increases, and in turn, their belief that it is meaningful grows.[10] When a leader provides clear purpose and goals, autonomy also increases productivity.[11] This does not mean organizational leaders should ignore subordinates and subordinate units or lose touch with their work. In fact, numerous studies have shown that leaders of successful groups keep tabs on performance without micromanaging.[12]

Operations vs. Organizations

Defining purpose with clarity is difficult for all leaders, but military leaders face the additional challenge of having to lead both active operations and standing organizations during their careers.

These are wildly different contexts, with diverse risks, rewards, challenges, and timeframes.

Military *operations* often have immediate feedback, with high stakes and tangible results. In such situations, it is incumbent on leaders to convey clear and meaningful purpose. Accordingly, military doctrine states that the commander's intent must include clear purpose:

A clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned.[13]

Surprisingly, however, for military *organizations* there is no comparable doctrine on the development and

communication of clear and meaningful organizational purpose. Without a clear purpose, the default view of "success" risks becoming "staying out of trouble," with little thought given to ultimate operational or strategic impact. Such commands come to exemplify compliance command,[14] wherein boxes checked become the markers for success. Navy Chief Information Officer Aaron Weiss stated, "We have a culture of compliance when it comes to [cyber] security. That culture leads people to say, 'If I do the checklist and I do all the right things . . . someone will give me a stamp that says I have authority to operate and I am secure.' [They miss the point that] security is a constant state of readiness."[15]

Compliance command stands in stark contrast to mission command, which encourages intelligent initiative toward a purpose within the bounds of commander's intent. While mission command generally is considered in relation to the

operational environment, its tenets are applicable—even critical—to all high-performing organizations. While serving as Army Chief of Staff, General Mark Milley explained, "We preach mission command, but we don't necessarily practice it on a day-to-day basis in everything we do. If we're going to have to operate like that in warfare, we have to train as we're going to fight. We have to live and operate like that on a day-to-day basis, even on daily administrative tasks you have to do in a unit area."[16]

In other words, "in-garrison mission command," as Darrell Frawley has termed it, will deliver both organizational and operational benefits because what happens upstream affects what happens downstream.[17] When guided by a shared purpose, any organization becomes more innovative, cohesive, and effective.

Another way in which operations and organizations ought to be alike but often are not concerns who gets to declare purpose. In most operations, the purpose is not determined by the team members or even their leader. Often expressed as commander's intent, purpose is assigned by someone further up the chain of command. However, in many standing organizations, incoming leaders are encouraged to put their own stamp on the mission statement. This misses the point. An organization's mission does not change just because its leader does. New leaders must address how best to accomplish their unit's purpose—not how to devise a different, more interesting, or more self-expressive purpose.

Across a variety of organizational improvement efforts in the military, including a recent study the authors contributed to on Air Force squadron vitality, we asked organizational leaders at all levels to describe the purpose of the units they lead.[18] Many had difficulty answering the question. Most commonly, these leaders recited only their unit's activities or duties, even when pressed for the larger, unspoken why of their work. Also common was dismissal of the question, with comments such as "it's obvious" or "it's self-evident," with no further elaboration, or "we all know our mission, so there's no need to discuss it." We also heard lofty descriptions of purpose that are too nondescript to be of much value, such as "we're here to defend our country." That is surely true, but it reveals little understanding of a unit's distinct part in that noble aim.

Finally, some leaders conflated their responsibilities as a leader with the purpose of the unit they led. They described their unit's purpose as something like "to take care of our members by creating an atmosphere that supports them and their families." While this is a good thing to do and helpful to the overall success of the team, it is not the purpose or critical outcome of the unit. It is not *why* the unit exists.

Fortunately, quite a few leaders can describe the purpose of their unit and appreciate the importance of its clarity. One Air Force security forces squadron commander explained, "Our purpose is about 'no harm': No harm to people, and then no harm to our assets. If we're talking about nuclear assets, then that priority is reversed," that is, smart, succinct, easily understood—and verifiable.

What Leaders Can Do

The Air Force study cited earlier, in addition to the authors' other work across the Services, has afforded an opportunity to learn from leaders who lead with clear and meaningful purpose. Here are some lessons from observations of those effective leaders.

Know the Unit's Purpose. Answering the question, "Why do we exist?" is devilishly hard, even though the resulting answer is usually simple. Organizational leaders who are able to answer that question usually come to it in one of two ways: deductively or inductively.

The deductive approach starts broadly and works toward specifics. For example, a leader may deduce a unit's overarching purpose by considering what problem(s) its standup aims to solve for its superior organization. Clues can also be gathered by considering what problems the unit ideally ought to solve for downstream supported organizations. This approach works because organizations are stood up to solve problems or meet challenges for people outside the organization. That outward-facing benefit is always the organization's purpose.

But the deductive approach is not for everybody. Especially for people quite close to the work of an organization, it might be easier to use the inductive approach—inferring purpose from activities. For them, the question to answer is, "Given the unit's primary tasks, what must its purpose be?" Based on the answer, leaders then can determine how best to state that purpose clearly. With this clarity, they return to their unit's tasks and determine what things it ought to do and ought not to do, revising based on a clearer view of purpose.

Both approaches can work, and success usually involves a combination of both: comparing forest to trees and back again until both the forest and the trees make sense and the purpose can be expressed in a clear and verifiable way.

Communicate Purpose Often and in Different Ways. Communicating organizational purpose means not only ensuring every team member knows the unit's purpose but also inspiring them to care about that purpose and to want to play a role in fulfilling it. As anthropologist-philosopher Gregory Bateson famously stated, "The meaning of your communication is the response you get."[19] Team members must believe, act on, and be willing to sacrifice based on that message. To that end, two aspects of communication are worth considering: variety and frequency.

Most new commanders determined to convey their unit's purpose would get high marks for variety during their first few weeks. They include the purpose in a short speech during their first commander's call, they put it on signs in hallways, they include it in guiding documents such as project charters and mission statements, and they put it under their email signature blocks. But the effort must be ongoing.

People need to be reminded that they are contributing to a meaningful purpose and, because of that, that they and their contributions are meaningful, too. *Creative redundancy*—making the same, important point repeatedly, but in a variety of ways and contexts—is an
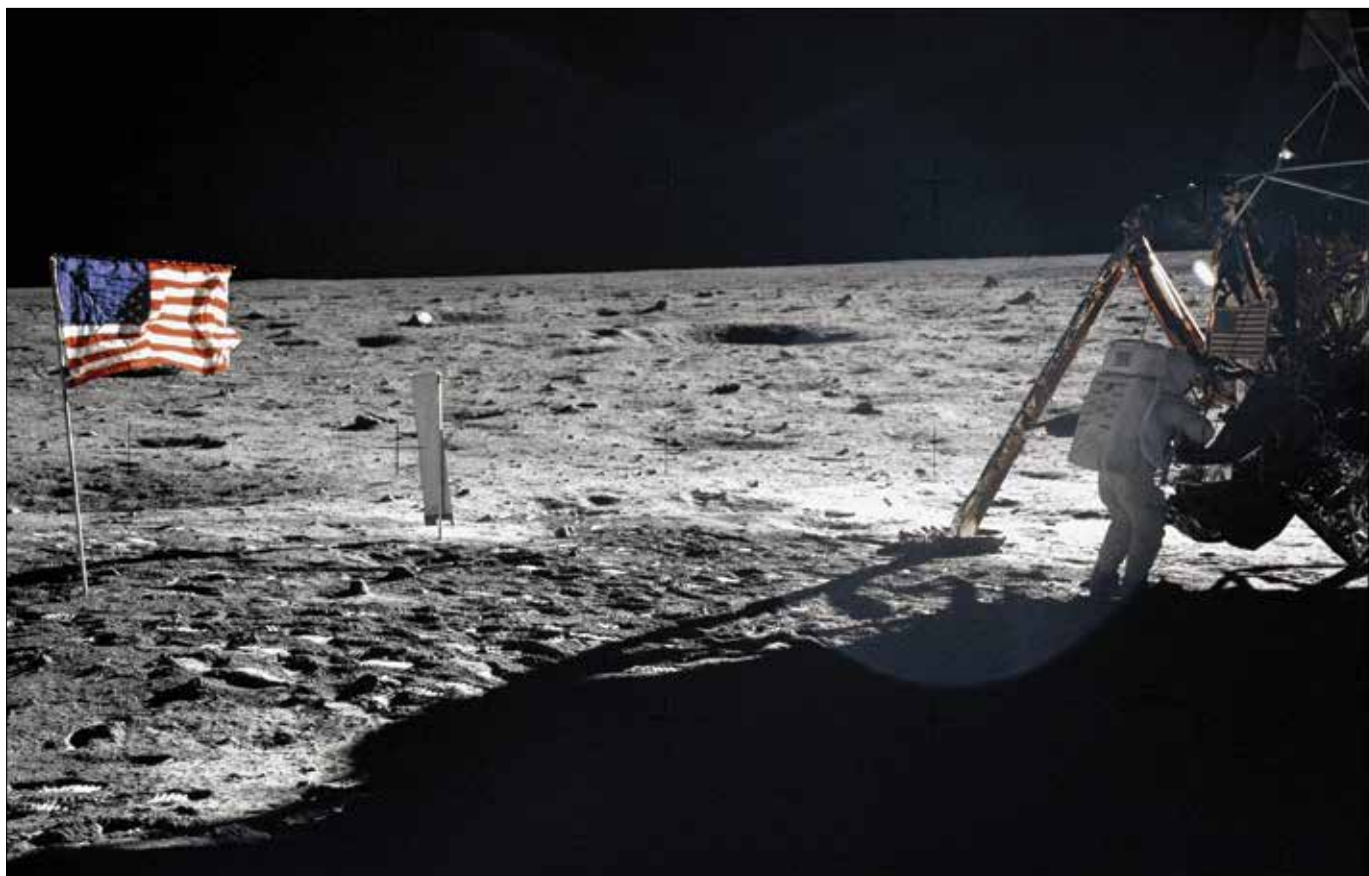
Buzz Aldrin's photograph of Apollo 11 landing site captures mission commander Neil Armstrong on lunar surface, July 20, 1969 (NASA)

essential tool of effective leaders. These leaders never forgo an opportunity to revisit a central theme, to use an occasion, a success, or a failure to emphasize the things they care about and want subordinates to care about, too. This is not the same as merely using a slogan or story again and again. It is about creating a cycle between daily articulation of purpose and refining and amplifying performance based on that purpose. It is a big job that requires a leader's attention from the first day on the job to the change of command.

Make It Personal. Nonoperational organizations exist to support or enable operations, and their effectiveness is critical, but they are removed in time and place from military victory. That is why effective organizational leaders work hard to help subordinates see the golden thread between their sometimes-mundane tasks and the contribution of those tasks to the greater good. This leadership task demands framing or tailoring the message to the audience or the individual.

The Air Force security forces commander mentioned earlier—the one who understood his unit's purpose—recounted this conversation with a bored security forces Airman: "If you let someone through the gate without proper ID, what might happen?" The Airman shrugged and admitted a possible bad result, but the commander kept digging. "And if that happened, what might happen? And then what? And then?" The Airman got the point, one domino at a time, and finally saw how her often-tedious task contributed to a weighty and worthy purpose. Her job was not always interesting. That did not change. What did change was her personal connection to the good she does—making a powerful difference to the people and property she cares for. Many successful leaders have had some version of that conversation: a time when they entered a subordinate's frame of reference to help him or her see how his or her work fit into something greater.

One well-known technique is to have support personnel spend time with the people they are supporting.[20] Parachute riggers, for example, would benefit from meeting the operators who will use the chutes. Administrative personnel, who often are behind the scenes, might feel stronger ownership of the mission if they are shown around the ship or across the base where their customers reside, or if they are included in unit functions. Even the smallest acknowledgment from the people being supported can refuel a sense of purpose. Support jobs are high-leverage positions, but like a physical lever, much leverage resides far from the load—making it hard to see one's relevance and impact. It is a leader's job to help subordinates bridge that gap.

Reinforce with Actions. There is much a leader can do beyond talk to reinforce a unit's clear and meaningful purpose. Actions based on purpose will elevate a unit's stated purpose from rhetoric to reality. Following are four of the most powerful ways to do that.

Anchor Key Measures to Purpose.
Measuring something is one way to convey that it is important, especially if any sort of consequence—positive or negative—is attached to the metric. That can be good news or bad, depending on what gets measured. Our study of Air Force squadron vitality revealed that many units succumb to the temptation to measure what is *easy* to measure instead of what is *important* to measure, thereby sending the wrong message. In other words, achievement of a unit's tasks often is easier to measure than achievement of its purpose (see figure).[21] Test scores, awards, or other proxies for achievement can lure leaders to focus on easily verified tasks when they may not be central to the unit's purpose. Measuring success based on compliance items such as ancillary training, fitness assessments, and the like is easy and may have to be done, but it cannot be allowed to overshadow success at delivering the unit's purpose.

For example, imagine a training command charged with providing a leadership course. A central purpose of such a course might be for the course's students to demonstrate certain new leadership skills on the job. But measuring that outcome would require surveying or interviewing students' bosses, which is troublesome. That measurement falls into the important-to-measure but hard-to-measure category. Easier would be to check off all the material being covered and to survey students' satisfaction with the class before they depart. That might yield useful information, but it would not tell instructors whether they were having the desired impact. In fact, it might tilt course design away from the course's intended impact.

Make Overt, Purpose-Based Decisions.
The leader reinforces purpose by referencing it when deciding how to allocate the unit's time, money, or energy. Purpose becomes the repeated and explicit touchstone for deciding, "What shall we do?" and "What shall we *not* do?"

Give Purposed-Based Feedback.
Well-delivered feedback both teaches and motivates. However, when

Figure. Achievement of Task Easier to Measure Than Purpose
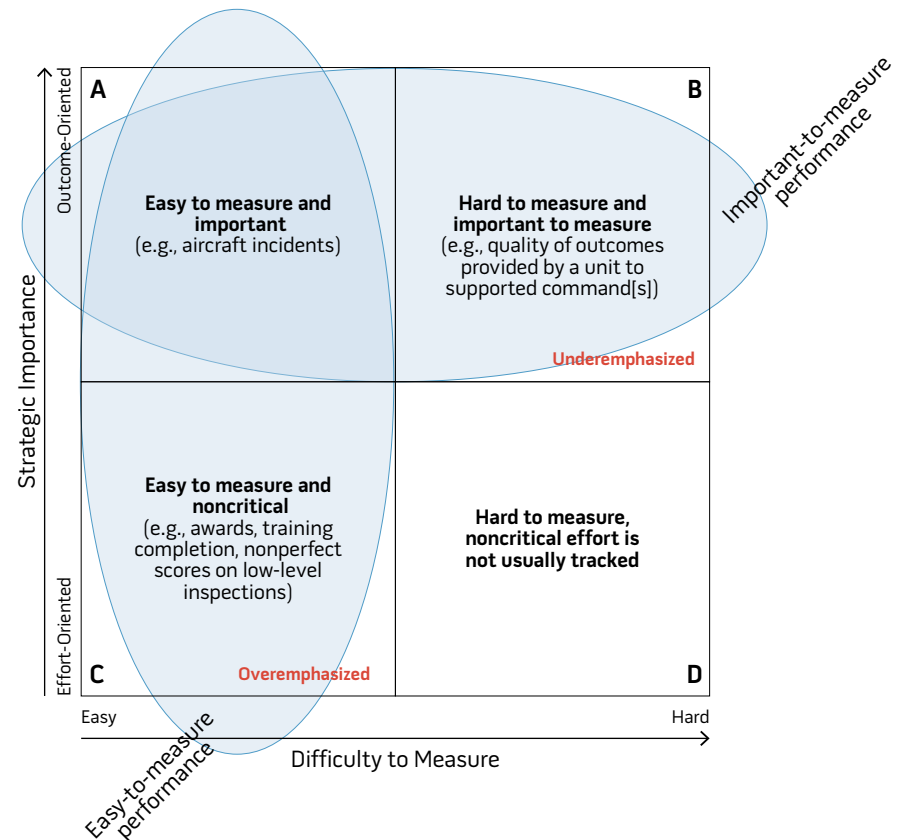
purpose is the point of reference for feedback, some additional benefits accrue: Performance on the thing that matters—that is, purpose—improves and understanding of the purpose improves.[22] If leadership guru Ken Blanchard is right that "feedback is the breakfast of champions," then purpose-based feedback is the breakfast of Olympians.

Align One's Own Behavior to Purpose. Subordinates are highly attuned to "glimpses of truth"—those brief moments that reveal the congruence between leaders' public personae and who they really are. An exquisitely articulated purpose understood by everyone means nothing if, in a glimpse of truth, subordinates see that the boss does not believe it or, worse, that the boss believes it does not apply to himself or herself. This usually happens when doing the right thing is also doing the hard thing. Walk the talk; it takes only a few missteps to hollow out a purpose that would uplift and direct the unit.

Leaders of military organizations must not become so distracted by the flood of daily activity that they forget—or allow their teams to forget—the point of all that activity. Clear and meaningful purpose helps teams pull together and in the right direction. *Clarity* speaks to the head, elevating decisionmaking by providing the context to make smarter decisions based on common aims. *Meaningfulness* speaks to the heart, elevating motivations and commitment. To provide both, leaders must know, communicate, and reinforce their unit's purpose. In every operation and every organization—large and small, temporary or ongoing—team members benefit when they see the point of their work, why it is important, and how they fit in to their organization's clear and meaningful purpose. The Nation then benefits when military units, whether in the action or supporting it, predictably fulfill their purpose. **JFQ**

Notes

[1] Stephen B. Knouse, *Keeping "On Task": An Exploration of Task Cohesion in Diverse Military Teams* (Patrick Air Force Base, FL: Defense Equal Opportunity Management Institute, Directorate of Research, Summer 1998), available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a359547.pdf>; Stephen B. Knouse, "Task Cohesion: A Mechanism for Bringing Together Diverse Teams," *International Journal of Management* 23, no. 3 (September 2006), 588.

[2] Carl E. Larson and Frank M.J. LaFasto, *Teamwork: What Must Go Right/What Can Go Wrong* (Washington, DC: SAGE Publications, 1989), 27.

[3] Quoted in Viktor Frankl, *Man's Search for Meaning* (Boston: Beacon Press, 2006).

[4] W.F. Cascio, "Changes in Workers, Work, and Organizations," in *Handbook of Psychology*, vol. 12, *Industrial and Organizational Psychology*, ed. W.C. Borman, D.R. Ilgen, and R.J. Klimoski (New York: John Wiley & Sons, 2003), 401–422.

[5] Daniel H. Pink, *Drive: The Surprising Truth About What Motivates Us* (New York: Riverhead Books, 2011).

[6] Catherine Bailey and Adrian Madden, "What Makes Work Meaningful—Or Meaningless," *MIT Sloan Management Review*, June 1, 2016, 53–61.

[7] "Vision, Mission, Values," Defense POW/MIA Accounting Agency, available at <www.dpaa.mil/About/Vision-Mission-Values/>.

[8] Andrew M. Carton, "'I'm Not Mopping the Floors, I'm Putting a Man on the Moon': How NASA Leaders Enhanced the Meaningfulness of Work by Changing the Meaning of Work," *Administrative Science Quarterly* 63, no. 2 (June 2018), 323–369, available at <https://doi.org/10.1177/0001839217713748>.

[9] Edwin A. Locke and Gary P. Latham, "New Directions in Goal-Setting Theory," *Current Directions in Psychological Science* 15, no. 5 (2006), 265–268, available at <http://doi.org/10.1111/j.1467-8721.2006.00449.x>.

[10] Yizhak Fried and Gerald R. Ferris, "The Validity of the Job Characteristics Model: A Review and Meta-Analysis," *Personnel Psychology* 40, no. 2 (June 1987), 287–322.

[11] Erik Gonzalez-Mulé et al., "Channeled Autonomy: The Joint Effects of Autonomy and Feedback on Team Performance Through Organizational Goal Clarity," *Journal of Management* 42, no. 7 (November 2016), 2018–2033, available at <https://doi.org/10.1177/0149206314535443>.

[12] Judith L. Komaki, *Leadership from an Operant Perspective* (London: Routledge, 1998).

[13] Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, October 22, 2018), 7.

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 1-0, *Personnel Support*

JP 2-0, *Joint Intelligence*

JP 3-0, *Joint Operations*

JP 3-03, *Joint Interdiction*

JP 3-36, *Joint Air Mobility and Sealift Operations*

JP X-XX, *Information*

JPs Revised (signed within last 6 months)

JP 1, *Doctrine for the Armed Forces of the United States, Vols. 1 and 2*

JP 3-05, *Special Operations*

JP 3-26, *Combating Terrorism*

JP 3-72, *Joint Nuclear Operations*

JP 3-85, *Joint Electromagnetic Spectrum Operations*

JP 5-0, *Joint Planning*

[14] Stephen L. Davis and William W. Casey, "A Model of Air Force Squadron Vitality," *Air & Space Power Journal* 32, no. 4 (Winter 2018), available at <www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-4/SLP-Davis_Casey.pdf>; Stephen L. Davis et al., *Improving Air Force Squadrons—Recommendations for Vitality: Report to the Chief of Staff of the United States Air Force* (Washington, DC: Headquarters Department of the Air Force, 2018), 46.

[15] John M. Doyle, "'Compliant' Doesn't Mean Secure, Navy CIO Says," *Seapower Magazine*, January 24, 2020, available at <https://seapowermagazine.org/compliant-doesnt-mean-secure-navy-cio-says/>.

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

[17] Darrell Frawley, "Mission Command in Garrison," in *Mission Command: The Who, What, Where, When and Why: An Anthology*, ed. Donald Vandergriff and Stephen Webber (CreateSpace Independent Publishing Platform, 2017), 121.

[18] Davis et al., *Improving Air Force Squadrons*.

[19] Gregory Bateson, *Steps to an Ecology of Mind: Collected Essays in Anthropology, Psychiatry, Evolution, and Epistemology* (Chicago: University of Chicago Press, 2000).

[20] Adam M. Grant, "Leading with Meaning: Beneficiary Contact, Prosocial Impact, and the Performance Effects of Transformational Leadership," *Academy of Management Journal* 55, no. 2 (April 2012), 458–576.

[21] Davis et al., *Improving Air Force Squadrons*, 60.

[22] Gonzalez-Mulé et al., "Channeled Autonomy."

The Importance of Joint Concepts for the Planner

By James L. Cook

Lieutenant Colonel James L. Cook, USA (Ret.), is a Professor of National Security Affairs at the U.S. Naval War College.

The 2018 National Defense Strategy explains the importance of developing new operational concepts to "sharpen our competitive advantages and enhance our lethality" across the entire spectrum of conflict.[1] The strategy forces us to think beyond military modernization and order of battle to consider how the joint force could be used in new and more effective ways in a future security environment that is "always in flux" and fraught with relentless change.[2] According to the Joint Staff, the purpose of joint concepts is to offer "alternative operational methods and related capabilities to maintain military advantage against current and emerging threats."[3] These concepts also propose necessary changes for the joint force to improve its ability to fight and win across all warfighting domains in these future conflicts.

David Fastabend argued that concepts provide innovative ideas intended, in part, to facilitate a debate that is the analytical "crucible" to identify flaws and generate consensus while adding a sense of clarity about the way ahead.[4] Simply put, he saw value in the joint concept development process that offers a collaborative framework to balance creative thinking with reality. Conversely, Antulio Echevarria contends that operational concepts are no panacea and have downsides. His criticisms include a "paradox," where the joint concept development

Air Force fighter jet flies overhead as two Soldiers raise signal tower for Patriot missile system during training exercise at Kadena Air Base, Japan, November 22, 2017 (U.S. Army/Adan Cazarez)

process itself is often impeded by Service biases and the absence of sustained commitment from the relevant stakeholders, which, in turn, means opportunity costs in the form of exploring other ideas.[5]

These differing views raise questions about the continued relevancy of joint concepts—and whether this approach is the most effective way to integrate advanced technology and other emergent capabilities into the joint force. This article argues that joint concept development is a critical, if underappreciated, component of military strategic and operational planning that is not currently being maximized to address emerging challenges and opportunities. To substantiate this premise, the article discusses the evolution of joint concepts and their influence on military planning today; describes the Joint Staff process in which concepts drive the development of required capabilities; and recommends some specific areas where joint concept development should be targeted going forward.

A Brief History

The Armed Forces have a proven track record of using strategy to inform the development of joint concepts that "address gaps, shortfalls, or inadequacies in existing approaches and capabilities," while presenting new ways to accomplish a joint operation, function, or activity.[6] An often cited example is the 1982 AirLand Battle concept that was conceived in the post–Vietnam War era to fill what Douglas Skinner called a "doctrinal vacuum."[7] It offered a new way to think about implementing the Cold War strategy of "containment" and defeating the Soviet Union. The Army's Training and Doctrine Command (TRADOC) Commander General Donn Starry was the driving force behind AirLand Battle, which applied some of the valuable lessons learned from the 1973 Arab-Israeli War and emphasized the importance of early offensive action and combined arms operations to winning the fight.

Army Field Manual (FM) 100-5, *Operations*, published in 1976, introduced the concept of active defense, which was designed to allow U.S. forces to fight outnumbered in Central Europe. Active defense emphasized the importance of winning the "first battle"[8] to provide time for reconsolidation before the next echelon of Soviet forces came within range.[9] David Johnson describes the dissatisfaction within the Army over the FM's emphasis on the defense at the expense of the offense. Moreover, he explains how Starry found the doctrine inadequate to solve the problems he faced as a corps commander against the Warsaw Pact, especially at the operational level of war.[10] The intra-Service doctrinal debates over the controversial active defense concept allowed for introspection and shaped the thinking of TRADOC and its schools.

The outcome of these intellectual efforts was the development of the AirLand Battle concept. FM 100-5 (1982) states

that AirLand Battle is based on "securing the initiative as early as possible and exercising it aggressively" by using synchronized air and ground operations, bold maneuver, and tempo to defeat a numerically superior Soviet military threat.[11] The concept also encouraged the employment of combined arms task forces (for example, armor and mechanized infantry units within the same formation) intended to create synergy and "pose a dilemma for the enemy."[12] Moreover, AirLand Battle was designed to bridge the gap between military strategy and tactics by focusing on the operational level of war using an extended deep, close, and rear battlefield framework; its requirement of a level of "jointness" in its implementation would later be expanded and codified in the 1986 Goldwater-Nichols Department of Defense Reorganization Act.

AirLand Battle also provided an intellectual foundation for Army modernization efforts during the so-called Reagan defense buildup in the early 1980s that procured mobile, lethal weapons systems including the M1 Abrams main battle tank, the Bradley infantry fighting vehicle, the Multiple Launch Rocket System, the PATRIOT air and missile defense system, and the Apache attack helicopter.[13] The capabilities provided by these advanced systems were critical for successful execution of the concept and validated by the U.S. military's performance during Operation *Desert Storm* in 1991. It is noteworthy that all of these "legacy" weapons systems remain in service today.

Joint Vision (JV) 2010 offered a capstone "conceptual template" that explained how the Armed Forces would "channel the vitality and innovation of our people and leverage technological opportunities" to improve joint warfighting effectiveness in the post–Cold War era.[14] JV 2010 was written to support President Bill Clinton's 1996 National Security Strategy that required the military to field forces "sufficient, in concert with regional allies, to defeat aggression in two nearly simultaneous major regional conflicts."[15] To advance the National Security Strategy and promote U.S. national interests, the 1997 National

Military Strategy required the joint force to shape the international environment, respond to the full spectrum of crises, and prepare now for an uncertain future.[16] To implement this strategic guidance, JV 2010 introduced four operational concepts—dominant maneuver, precision engagement, full-dimension protection, and focused logistics—enabled by information superiority to mass effects and achieve "full spectrum dominance" across the entire range of military operations.[17]

With the benefit of hindsight, JV 2010 was far from prescient in its assessment of the future security environment, and its shortcomings include an overreliance on technology and insufficient attention paid to operations other than war, such as counterterrorism and counterinsurgency operations. That said, the document was an effective medium to emphasize the importance of becoming "fully joint: institutionally, intellectually, and technically."[18] Moreover, JV 2010 influenced institutional changes for the Services and guided efforts to improve joint warfighting and the procurement of advanced capabilities including intelligence, command and control, precision-guided munitions, and air and missile defense, which are all critical to the joint force today. On balance, JV 2010 did a creditable job preparing military strategists and operational planners to confront the challenges of a new millennium, while deeply influencing and shaping today's joint force.

Finally, in 2003, the Department of Defense (DOD) published the Joint Operations Concept (JOPSC) as a "unifying framework" to guide Secretary of Defense Donald Rumsfeld's transformation efforts for the Armed Forces in a post-9/11 world where "adapting to surprise—adapting quickly and decisively—must . . . be a condition of planning."[19] He also articulated the requirement to "transform not only our Armed Forces but also the Defense Department that serves them—by encouraging a culture of creativity and intelligent risk-taking."[20] The JOPSC echoed JV 2010's emphasis on the importance of achieving full-spectrum dominance, but it advocated a

capabilities-based approach "that focuses more on how the United States can defeat a broad array of capabilities that an adversary may employ rather than who the adversaries are and where they may engage U.S. interests."[21] In both cases, the need for new concepts occurred in response to abrupt changes in the security environment following the collapse of the Soviet Union in 1991 and the terrorist attacks against the United States in 2001.

How Are Concepts Used Today?

JV 2010 and JOPSC were replaced by the 2012 Capstone Concept for Joint Operations (CCJO), which was intended to guide joint force development—after a decade of combat operations in Afghanistan, Iraq, and Syria—toward a more potentially dangerous world that includes the reemergence of "long-term strategic competition" with China and Russia and the proliferation of advanced technologies.[22] The CCJO describes the Chairman of the Joint Chiefs of Staff's vision for how the joint force of 2020 will "defend the Nation against a wide range of security challenges" consistent with defense strategic guidance provided in the 2012 *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* The guidance required a "rebalance" from the post-9/11 "war on terror" waged against al Qaeda and other terror groups primarily on land toward the Asia-Pacific with its different set of challenges, including a largely maritime environment.[23]

In practice, the capstone concept serves as a "bridge between strategic guidance and joint operating concepts in support of joint force development."[24] For example, the 2012 CCJO introduced an approach called Globally Integrated Operations (GIO), which calls for elements of the joint force that are globally postured to "combine quickly with each other and mission partners to integrate capabilities fluidly across domains, echelons, geographic boundaries, and organizational affiliations."[25] This approach aligns with the 2018 National Defense Strategy's emphasis on "strategic flexibility" and "freedom of action" in its description of dynamic force

Table. DOD Capability Framework

Doctrine	While not authoritative, joint concepts should consider existing doctrine and propose clear alternatives to these "fundamental principles" that guide the employment of U.S. military forces where appropriate.
Organization	Joint concepts may require changes in the way the joint force organizes to accomplish assigned missions. This may include creating new—or modifying extant—organizations and force structure.
Training	While joint doctrine is the basis for joint training, some joint concepts may require adopting new and innovative approaches to training exercises and other events across the full range of joint functions or missions.
Materiel	As described earlier, joint concepts propose capabilities to improve the ability of the joint force to address future security challenges. Once approved, the recommended materiel capabilities (for example, weapons systems) may result in validated military requirements through the Joint Capabilities Integration and Development System.
Leadership and Education	Joint concepts may provide the basis for new courses of study across the professional military education enterprise. These classroom discussions encourage critical thinking about the joint concept and support the further development of new ideas.
Personnel	The successful implementation of a joint concept may require members of the Armed Forces to acquire new individual and collective skills. These changes may affect recruitment, retention, and the professional development of the joint force.
Facilities	Joint concepts may affect the size, type, and number of facilities required in and outside of the continental United States, for deployment, reception, staging, movement, integration, and sustainment.
Policy	Joint concepts and policy are closely related. Because policy can direct or assign tasks, prescribe desired capabilities, and provide guidance, concept developers should consider and account for current policy when proposing new or alternative ways in which the joint force could operate.

Source: Chairman of the Joint Chiefs of Staff Instruction 3010.02E, *Guidance for Developing and Implementing Joint Concepts* (Washington, DC: The Joint Staff, August 17, 2016), A-3–A-5.

employment, which is intended to provide more options for priority missions while introducing "unpredictability to adversary decisionmakers."[26] Finally, the CCJO establishes priorities that implement the Chairman's high-order vision and guide the development of a family of more specific and detailed subordinate joint operating and supporting concepts.

Joint operating concepts (JOCs) are broadly defined as describing "how the joint force may execute military operations within a specific military mission area in accordance with defense strategic guidance and the CCJO."[27] As an example, the Joint Operations Access Concept (JOAC) is a "warfighting concept" that explains—in conceptual terms—how the joint force would achieve and maintain operational access "in the face of armed opposition by a variety of enemies and under a variety of conditions, as part of a broader national approach."[28] It allows Service planners to determine the contributions and limitations of their respective forces under specific scenarios. For instance, the concept recognizes that air superiority and sea control—advantages that U.S. forces have enjoyed for decades—are no longer assured.

The JOAC addresses operational access consistent with the guidance and context provided by the CCJO,[29] while directly addressing the *Sustaining U.S.*

Global Leadership requirement to "project power despite antiaccess/area-denial (A2/AD) challenges."[30] One can envision the JOAC's application in response to a crisis in the South China Sea or other global maritime hotspots. The concept's central idea is to leverage cross-domain synergy "to establish superiority in some combination of domains that will provide the freedom of action required by the mission."[31] Additionally, the JOAC identifies 30 required capabilities and 11 operational access precepts (that is, general principles) intended as a "guide to judgment" based on an understanding of the unique factors of any situation.[32]

While critics argue that the JOAC lacks necessary detail for such a complex military problem, it is important to understand that this document provides an "overarching concept" under which can "nest" multiple supporting concepts, such as the Joint Concept for Entry Operations (JCEO), that address specific aspects of A2/AD challenges. Supporting concepts add depth and detail to JOCs by describing how the joint force may conduct a particular subset of the mission.[33] In this case, the JCEO focuses on integrating force capabilities across domains "in order to secure freedom of maneuver on foreign territory *within* an operational area" that is consistent with the GIO approach.[34] Specifically, JCEO seeks to employ

maneuver in and across multiple domains to establish local superiority at multiple entry points to gain access and achieve military objectives.[35] The document lists 21 required capabilities and affirms the need for the joint force to maintain its ability to enter foreign territory and accomplish all assigned missions ashore, both in the littoral regions and farther inland.[36]

In sum, the Joint Staff provides a logical, hierarchical process that translates strategic direction into proposed solutions for the joint force in the future security environment. Developing joint operating and supporting concepts—with GIO as a guide—gives intellectual focus and creativity to address specific mission areas and challenges. Moreover, the aforementioned collaborative nature of concept development facilitates engaging relevant stakeholders in the discussion—with a goal of enhancing the effectiveness and lethality of the joint force.

The Services formulate concepts that align with the broader joint concepts, while focusing on their unique contributions and Title 10 responsibilities to "organize, train, and equip" forces for joint and combined operations. For example, in 2014, the Army released *The Army Operating Concept: Win in a Complex World*, which describes its support for GIO by providing

"foundational capabilities required by the joint force." The Army also plans for and executes expeditionary operations consistent with the JOAC and JCEO by "integrating with other Services and mission partners to conduct joint combined arms maneuver [and] the synchronized application of capabilities critical to accomplish the mission."[37] In response to the CCJO requirement for the joint force to "integrate capabilities fluidly across domains," then–Army Chief of Staff General Mark A. Milley testified before Congress that the Army's Multi-Domain Operations concept is designed to "guide our modernization efforts . . . inform future force development through numerous iterations of experimentation and analysis . . . [and] describe how we will synchronize our capabilities across all domains in support of the joint force."[38]

Despite the importance of operational concepts to the planning process, Echevarria correctly argues that they are "usually poorly defined in military doctrine or shrouded in jargon, which in turn leads to confusion."[39] For example, what is the difference (if any) between a joint concept, an operating concept, and an operational concept? The ambiguity is more than a mere semantics issue and should be clarified by the Joint Staff for military strategists and operational planners. In the interim, how does one select the right concepts? To be clear, these choices can at times seem more art than science given the wide array of possible threats across the spectrum of conflict. Nevertheless, prudent concept development starts with an assessment of the future security environment to identify challenges and opportunities, followed by a thorough review of strategic direction to understand the context and consider potential capability deficiencies or other obstacles.

Once written, concepts are an important element of scenario-based planning to measure the joint force's ability to succeed in realistic situations, as they also identify capability gaps and other shortcomings. Evan Braden Montgomery argues that scenarios are "not intended to be predictions of the future" but are instead "stories about the way the world might turn out tomorrow . . . that can help us recognize and adapt to the changing aspects of our present environment."[40] As an example, he offers a scenario that describes a potential Sino-U.S. conflict in the Taiwan Strait to facilitate the assessment of operating concepts such as the JOAC and JCEO against a specific A2/AD challenge while mitigating risk. This scenario could also be used to address important joint and Service capability issues such as the employment of aircraft carriers and manned versus unmanned systems in such a challenging environment.

From Concepts to Capabilities

The 2030 Capstone Concept for Joint Operations describes a shift to a "joint concept–driven, threat informed capability development process" intended to drive the Pentagon's resource allocation decisions.[41] Although some view the term *capabilities* through the relatively narrow lens of weapons systems, DOD and the Joint Staff take a more holistic view. Joint Publication 1, *Doctrine for the Armed Forces of the United States*, states that joint concepts lead to military capabilities, both nonmaterial and materiel, that "significantly improve the ability of the joint force to overcome future challenges" and achieve strategic and operational objectives.[42] This robust array of potential capability options to fill identified gaps is captured by the DOD acronym DOTMLPF-P, which serves as an intellectual framework for institutional change (see table).

Conclusion and Recommendations

Mark Guzinger argues that "legacy" operational concepts based on favorable Operation *Desert Storm*–like scenarios have hindered necessary changes in the past.[43] Fortunately, the 2018 National Defense Strategy emphasizes the need for fresh thinking and innovative approaches to increase the lethality and overall effectiveness of the joint force. This is both encouraging and necessary because an inclusive, transparent exchange of ideas is critical to look beyond the status quo and truly examine novel ways to address 21st-century security challenges that are increasingly transregional, multidomain, and multifunctional (TMM).

For example, the 2030 CCJO states that the joint force "will globally posture forces and prioritize readiness for major combat against peer competitors while providing options for proactive and scalable employment of the joint force anywhere in the world."[44] Given this guidance, what are future overseas basing requirements in a TMM environment, where response times to crises are shortened and managing escalation and joint force resiliency would be tested in myriad ways?[45] And how are combatant commands and the Services impacted? Formulating answers to these difficult questions should begin with operationalizing dynamic force employment through the development of joint concepts.

The 2018 National Military Strategy directs the joint force to successfully "compete below the level of armed conflict (with a military dimension)."[46] With the exception of cyberspace, this is a rather ambiguous mission area that requires some out-of-the-box thinking to address so-called gray zone or hybrid warfare challenges that exist in the space between peace and war.[47] How might the joint force respond to future attempts to employ "little green men," armed militias, disinformation campaigns, and other efforts to disrupt national sovereignty and stability? Given the complexity and the political implications of such operations, how can the military's efforts be integrated as part of a broader interagency effort?

Finally, how might the joint force integrate cutting-edge technology such as hypersonic weapons, quantum computing, and artificial intelligence to support GIO? The development of new joint concepts must embrace these emerging capabilities and harness their potential advantages to present "insurmountable dilemmas" for future adversaries.[48]

Perhaps some or all of these questions will be addressed in the forthcoming Joint Warfighting Concept (JWC), which intends to provide "a threat-informed capability development roadmap for

all-domain joint maneuver warfare."[49] Vice Chairman of the Joint Chiefs of Staff General John Hyten describes JWC as an "overarching concept" that will help guide the development of "capabilities and attributes that we need to be able to fight effectively in the 2030s and 2040s and beyond."[50]

Former Chairman of the Joint Chiefs of Staff General Joseph Dunford believes that "the strategic landscape is changing and our investment in future capabilities, capacity, and readiness must keep pace to ensure our men and women in uniform never face a fair fight."[51] Joint concepts are critical to this effort because they provide a narrative framework that incorporates a comprehensive assessment of the security environment and strategic direction to identify and prioritize existing shortfalls; at the same time, joint concepts propose innovative approaches and required capabilities to maximize the joint force's qualitative and quantitative advantages to solve complex problems. **JFQ**

Notes

[1] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense [DOD], 2018), 7.

[2] *Joint Operating Environment 2035* (Washington, DC: The Joint Staff, July 14, 2016), 1.

[3] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3030.01, *Implementing Joint Force Development and Design* (Washington, DC: The Joint Staff, December 3, 2019), C-2–C-3.

[4] David A. Fastabend, "That Elusive Operational Concept," *Army Magazine* 51, no. 6 (June 2001), 42.

[5] Antulio J. Echevarria II, "Operational Concepts and Military Strength," The Heritage Foundation, October 7, 2016, available at <www.heritage.org/military-strength-topical-essays/2017-essays/operational-concepts-and-military-strength>.

[6] CJCSI 3010.02E, *Guidance for Developing and Implementing Joint Concepts* (Washington, DC: The Joint Staff, August 17, 2016), A-1, A-3.

[7] Douglas W. Skinner, *Airland Battle Doctrine* (Alexandria, VA: Center for Naval Analyses, September 1988), 3.

[8] Field Manual (FM) 100-5, *Operations* (Washington, DC: Headquarters Department of the Army, 1976), 1-1.

[9] Martin J. D'Amato, "Vigilant Warrior: General Donn A. Starry's AirLand Battle and How It Changed the Army," *Armor* 109, no. 3 (May–June 2000), 19.

[10] David Johnson, "An Army Trying to Shake Itself from Intellectual Slumber, Part 1: Learning from the 1970s," *War on the Rocks*, February 2, 2018, available at <https://warontherocks.com/2018/02/army-trying-shake-intellectual-slumber-part-learning-1970s/>.

[11] FM 100-5, *Operations* (Washington, DC: Headquarters Department of the Army, August 20, 1982), 7-2.

[12] Ibid., 7-4.

[13] Kari Hawkins, "AMC-Developed Weapons Remain Vital to Army," *Army.mil*, September 6, 2012, available at <www.army.mil/article/86839/amc_developed_weapons_remain_vital_to_army>.

[14] *Joint Vision 2010* (Washington, DC: The Joint Staff, July 1996), 1.

[15] *A National Security Strategy of Engagement and Enlargement* (Washington, DC: The White House, February 1996), 14.

[16] *National Military Strategy: Shape, Respond, Prepare Now—A Military Strategy for a New Era* (Washington, DC: The Joint Staff, 1997), 1.

[17] *Joint Vision 2010*, 1.

[18] Ibid., 9.

[19] *Quadrennial Defense Review Report* (Washington, DC: DOD, September 30, 2001), iii.

[20] Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs*, May/June 2002, available at <www.foreignaffairs.com/articles/2002-05-01/transforming-military>.

[21] *Joint Operations Concept* (Washington, DC: DOD, November 2003), 9.

[22] *Summary of the 2018 National Defense Strategy*, 1.

[23] *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: The Joint Staff, September 10, 2012), 1.

[24] CJCSI 3010.02E, A-10.

[25] *Capstone Concept for Joint Operations: Joint Force 2020*, iii.

[26] *Summary of the 2018 National Defense Strategy*, 5, 7.

[27] CJCSI 3010.02E, A-10.

[28] *Joint Operations Access Concept (JOAC)*, Version 1.0 (Washington, DC: DOD, January 17, 2012), i.

[29] Ibid., 3.

[30] *Sustaining U.S. Global Leadership: Priorities for 21st-Century Defense* (Washington, DC: DOD, January 2012), 4.

[31] *JOAC*, ii.

[32] Ibid., 17.

[33] CJCSI 3010.02E, A-10.

[34] *Joint Concept for Entry Operations* (Washington, DC: The Joint Staff, April 7, 2014), v. Emphasis in original.

[35] Ibid., 10.

[36] Ibid., iii.

[37] U.S. Army Training and Doctrine Com- mand (TRADOC) Pamphlet 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World* (Washington, DC: TRADOC, October 7, 2014), 5.

[38] Senate Armed Services Committee, *Posture Statement by General Mark A. Milley, U.S. Army Chief of Staff*, 116th Cong., 1st sess., March 26, 2019, 5–6.

[39] Echevarria, "Operational Concepts and Military Strength."

[40] Evan Braden Montgomery, *Defense Planning for the Long Haul: Scenarios, Operational Concepts, and the Future Security Environment* (Washington, DC: Center for Strategic and Budgetary Assessments, 2009), 14–15.

[41] *Capstone Concept for Joint Operations: Joint Force 2030* (Washington, DC: The Joint Staff, June 18, 2019), v.

[42] Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 23, 2013, Incorporating Change 1, July 12, 2017), xxvi.

[43] Mark Guzinger, *Shaping America's Future Military Toward a New Force Planning Construct* (Washington, DC: Center for Strategic and Budgetary Assessments, 2013), 23.

[44] *Capstone Concept for Joint Operations: Joint Force 2030*, 4.

[45] Kathleen H. Hicks, "The Overseas Basing Debate, Part 1," Defense 2020 Podcast, transcript, Center for Strategic and International Studies, February 10, 2020, available at <www.csis.org/analysis/overseas-basing-debate-part-1>.

[46] *Description of the National Military Strategy 2018* (Washington, DC: The Joint Staff, 2018), 3.

[47] Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (2018), available at <www.jstor.org/stable/26542705?seq=1#metadata_info_tab_contents>.

[48] *Capstone Concept for Joint Operations: Joint Force 2030*, 7.

[49] Senate Arms Services Committee, Department of Defense Budget Hearing, *Statement of General Mark A. Milley, USA, 20th Chairman of the Joint Chiefs of Staff*, 112th Cong., 2nd sess., March 4, 2020, 12.

[50] Theresa Hitchens, "New Joint Warfighting Plan Will Help Define 'Top Priority' JADC2: Hyten," *Breaking Defense*, January 29, 2020, available at <https://breakingdefense.com/2020/01/new-joint-warfighting-plan-will-help-define-top-priority-jadc2-hyten/>.

[51] Senate Appropriations Committee on Defense, *Posture Statement of General Joseph Dunford, Jr., USMC, 19th Chairman of the Joint Chiefs of Staff*, 115th Cong., 1st sess., March 22, 2017.

Workers assemble B-25 bombers at North American Aviation, Kansas City, Kansas, October 1942 (Library of Congress/Alfred T. Palmer)

Mobilization in the 21st Century
Asking the Right Question

By Matthew C. Gaetke

A renewed focus on Great Power competition means major wars are getting attention again, and these kinds of wars consume a lot of resources. Historically, big wars required wartime industrial mobilization to produce all those resources. War mobilization conjures black and white images of tanks, planes, and ships pouring out of American factories during World War II. But does bringing these pictures to life reflect the realities of major war in the 21st century? Can we even make all those things? More important, is planning for this kind of industrial overhaul a high priority in preparing for a major war with a peer competitor? Is this even the right question?

Colonel Matthew C. Gaetke, USAF, is Special Assistant to the Director and Air Force Operational Liaison at the Defense Advanced Projects Research Agency.

This article analyzes the factors behind mobilizing U.S. industry to support a large modern war. But what is mobilization? U.S. joint doctrine broadly defines *mobilization* as "the process of assembling . . . national resources . . . in time of war."[1] This means, at least, massing people into uniform, leveraging industry to produce weapons and equipment, and sustaining public support for these measures.[2] It also requires generating the financial resources to pay for it all. Among these elements of mobilization, this article focuses on industry, the economy, and producing military equipment—and doing so when wartime demands exceed military industrial capacity. This is different from stockpiling in case of war, peacetime decisions over force size, rapid development of new technologies, and surging existing industry. Mobilization happens when these are not enough. Mobilization means converting a significant portion of the civilian economy to military production to generate the materiel necessary to fight a sustained major war.

The following sections show, first, that the contextual differences between World Wars I and II—wars that involved mobilization—and a war in this century make such mobilization unlikely. The belligerents of the world wars began them with roughly similar economic potential, which set the conditions for neither side being able to overwhelm the other. Since mobilization happens in relation to an adversary, among modern competitors only China could play this role. Second, unlike in the world wars, the United States would enter a 21st-century conflict already fitted with high-end military equipment in considerable quantity. There would be no need for the U.S. military to expand just to catch up, a driver of previous mobilizations. Overcoming previous American disarmament required a rapid expansion of military production into the civilian economy. While a 21st-century major war would certainly require increased military production, the increase would be considerably smaller and would not require widespread conversion of the civilian economy. Finally, projected combat losses in a war between the United States

and China further scope the industrial effort required. These loss rates, although sometimes exceeding current production rates, do not dwarf them. Today, production rates for some items already exceed estimated wartime loss rates.

Given this context, the United States is well postured to sustain a major 21st-century war without the kind of mobilization experienced in the world wars. Immense uncertainty, however, surrounds other aspects of such a war. Since the United States has not fought a peer war since Korea, characterizing this kind of future combat is guesswork. Furthermore, the United States has never fought a modern war with the homeland at risk, as it would be—at least through cyberspace—during even minor 21st-century wars. In the face of these unknowns, *how to mobilize* is the wrong question. How to develop the right options to prevail despite this uncertainty is far more important than fretting over re-creating the mobilization of World War II.

A Peer War Requires a Peer Competitor

A sustained major conflict that would drive mobilization requires closely matched adversaries in terms of military capability, productive capacity, and economic power. This is logical; significant differences in productive capacity would allow one side to outproduce the other without converting swaths of its civilian economy. Gross domestic product (GDP) is a proxy for the productive capacity of an economy and therefore gives a rough indication of its ability to sustain a major war. Examining the GDPs of the major powers from World Wars I and II shows what degree of difference might exist between adversaries' economies and yet still see them engage in the kind of sustained major war that involves mobilization. Filtering today's potential adversaries by that degree of difference—while having no political or military predictive ability—indicates how well their economies might be able to sustain such a war against the United States. Only a war with such a matched adversary might require the mobilization of the American economy.

Before World War I, the economies of the major powers were of comparable size, especially when measured by the alliance blocks that played a key role in the war. The figure shows the 1913 GDPs of the major powers (at purchasing power parity in 2011 dollars, showing how far government spending could go within each economy). The economies of most, such as the United Kingdom, were within a factor of two of the median. The Ottoman Empire was significantly less, and the United States significantly more. Grouping the economies by alliance block gives an even clearer picture of the prewar balance. Considering the initial combatants, the entente's GDP was 1.8 times larger than that of the Central Powers. On a smaller scale, as the Austrians issued an ultimatum that would start the war, they faced an adversary alliance with almost exactly the same GDP ($503 billion for Germany vs. $495 billion for Russia and Serbia).[3]

The World War II powers' GDPs were also comparable at the start. In 1938, their economic output was again within a factor of about two, with the United States again an outlier.[4] Only Italy was less than half, and the Soviet Union was more than twice the median (again the United Kingdom).[5] Separating the powers into alliance blocks, France and Britain faced continental adversaries Germany and Italy with an almost identical combined GDP. Including Japan and the United States would make the ratio 3.4 to 1 in favor of the Allies, but that is misleading. By the time the United States entered the war, France and portions of the Soviet Union were already producing—at lower levels—for the Axis. One estimate of the impacts of the early Axis gains puts the adjusted Allied GDP at about $1.44 trillion by 1942 to the Axis's $1.55 trillion, assuming full production from conquered areas.[6] That means a GDP ratio of between 1.1 and 2 to 1, depending on how effectively the Axis could convert the economic potential of captured workers and territory.

Together, the world wars suggest that adversaries with GDPs within a factor of about two are sufficiently comparable to allow for a sustained major war

and mobilization. Other 20th-century wars—those without American mobilizations—saw a very different degree of economic disparity between adversaries. As the United States entered the Korean War, American GDP (conservatively excluding allies) was 5.5 times greater than that of China and North Korea combined. In 1965, U.S. GDP was 95 times larger than that of North Vietnam.[7] In the Gulf War, the ratio was 71 to 1, again excluding the coalition.[8] It rose to 135 to 1 by 2002 for Operation *Iraqi Freedom*.[9] These cases where the GDP difference was greater than a factor of two included other forms of marshaling resources (activating Reserve personnel, leveraging Reserve lift, surging production, even creating specific acquisition programs like Mine-Resistant Ambush Protected vehicles), but not the widespread conversion of the civilian economy that is mobilization.[10]

How do today's potential adversaries stack up? American GDP is roughly $21 trillion as of late 2018, in current dollars.[11] At purchasing power parity (internal buying power of government spending), China's GDP is $23 trillion and Russia's is $3.8 trillion.[12]

Considering a future major war, though, requires estimating future GDPs. The U.S., Chinese, and Russian GDPs all grew in 2019, by 2.1 percent, 6.1 percent, and 1.3 percent, respectively, according to each government.[13] All three real GDP growth rates, however, show faster growth than each economy's long-term, potential GDP growth rate. Based on Conference Board estimates—comparable to Federal Reserve and Congressional Budget Office projections—U.S. potential GDP growth is just less than 2 percent, China's is close to 3 percent, and Russia's is essentially zero.[14] While actual GDP growth will fluctuate—COVID-19 throws a wrench in any projection—over the long term it should converge to the potential GDP growth rate.

All three rates are also slowing, but the U.S. growth potential is slowing the least quickly and shows the best prospects for stable growth.[15] For simplicity, projecting future GDP based on current

Figure. GDPs of Major Powers
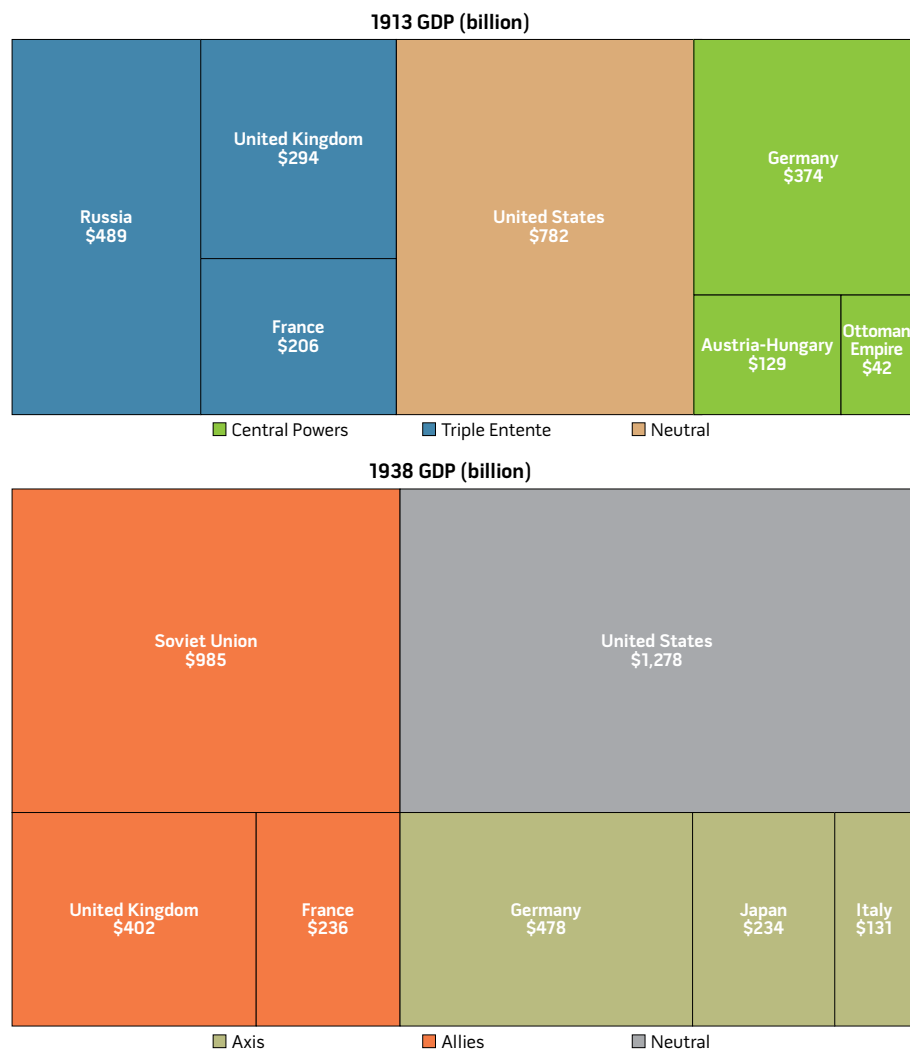
Sources: Stephen Broadberry and Mark Harrison, "The Economics of World War I: An Overview," in *The Economics of World War I*, ed. Stephen Broadberry and Mark Harrison (Cambridge: Cambridge University Press, 2005), 7–10. Updated gross domestic products (GDPs) per capita are from Maddison Project Database 2018, last modified January 25, 2018, as described in Jutta Bolt et al., *Rebasing "Maddison": New Income Comparisons and the Shape of Long-Run Economic Development,* Groningen Growth and Development Centre Research Memorandum 174 (Groningen, The Netherlands: Groningen Growth and Development Centre, January 2018).

potential GDP growth rates—ignoring rates of change of the growth rates or the immediate impact of the COVID-19 crisis—should therefore give a conservative estimate of U.S. advantage. If 2018 potential GDP growth rates were made actual to 2070, the U.S. economy would remain about the size of China's, but would be 34 times larger than Russia's. Meanwhile the sluggishness of the Russian economy has already impacted military purchases.[16] None of this accounts for allies—among which the United States counts some of the world's

largest economies, with no similar economic powerhouses likely to align with either China or Russia.

In summary, only China has the economic capacity to sustain a major war with the United States. Unfortunately, the seeds of such a war are all too easy to imagine. After promising in 2015 not to militarize its outposts in the South China Sea, China later installed antiship and antiaircraft missiles on several manufactured islands, threatening any ship passing between Vietnam and Brunei.[17] Taiwan also presents a potential flashpoint. On

Table 1. U.S. and China Militaries

	United States	China	U.S. Advantage	Sixty Percent, U.S. Advantage
Tactical Submarines	54	58	0.9	0.6
Major Surface Combatants	87	23	3.8	2.3
Aircraft Carriers	11	1	11	6.6
Fifth-Generation Fighters	303	6	50.5	30.3
Fourth-Generation Fighters	1,568	1,542	1	0.6
Fighters Total	1,871	1,548	1.2	0.7
Bombers	139	189	0.7	0.4
Personnel (Active and Reserve)	2,206,000	2,545,000	0.9	0.5

Source: "Chapter Three: North America," *The Military Balance* 118, no. 1 (2018), 46–63; "Chapter Six: Asia," *The Military Balance* 118, no. 1 (2018), 249–259.

January 2, 2019, Chinese President Xi Jinping reiterated that Taiwan "must and will" be united with mainland China.[18] A conflict would be easy to start and could easily escalate. A 2016 RAND study concludes that Sino-American tension has "a bias toward a long, severe, bitter war."[19] Such a war would demand more from American industry, but just because the economies will likely remain comparable does not mean it will require mobilization.

Mobilization to Catch Up

Despite their economies' relative sizes, the similarity of the American and Chinese militaries' sizes actually makes war mobilization less likely. Previous American mobilizations began as an effort to catch up to other powers. The situation is very different now. For the world wars, the military industrial base that supplied the prewar American military could not support the multifold military expansion required just to draw even. That growth meant converting large portions of the civilian economy to military production—that is, mobilization.

In 1913, the U.S. military was neither large enough nor well enough equipped to register as a peer competitor in Europe, using the number of military personnel as a proxy for quantity of military equipment and for military production capacity. The prewar U.S. military was several times smaller than those of the other powers,

one-fifth the size of Germany's and one-quarter the size of France's or the United Kingdom's.[20] It grew almost 19 times by 1918.[21] Even if the 1913 American military had been equipped with plentiful quantities of the best equipment—and it was not—this growth would have overwhelmed the industrial base that initially supplied it.[22] The problem turned out to be insurmountable. In fact, when the Doughboys made it to the front, they fought with weapons made in Europe.[23]

In 1939, the U.S. military was again much smaller than those of the European powers, only one-eighth the size of Germany's and one-third the size of Japan's.[24] If the United States alone had needed to fight the Axis powers, its military would have needed to grow by a factor of 13 just to be even.[25] In the event, it grew 36 times by 1945.[26] Once again, the industry supplying the American military in 1939 could not surge to equip one 36 times larger. Instead, the United States needed to convert large portions of its civilian economy to handle this growth. Mobilization was first an effort to catch up.

The situation is different today. Even three decades after the Cold War, despite an overall decrease in military spending relative to GDP, the United States still fields the world's most powerful military, and one of the largest.[27] By many measures, the United States has a numerically equivalent force to China's. In terms of total military personnel (Active plus Reserve), tactical

submarines, and nonstealthy aircraft, the Chinese and the American militaries are of similar size (table 1). The United States, however, has 11 aircraft carriers in comparison to China's 2 and a significant head start in stealthy, fifth-generation fighter aircraft. This article focuses on sea and air forces, anticipating a certain kind of Sino-American war and also simplifying the analysis to focus on big-ticket platforms. This method would also apply to a large army engaged in a major land war with China, but the logic of such a war is less clear.

On the other hand, the United States has global responsibilities, in contrast to China's regional focus, and must always balance the risk from other threats. The RAND study projected that the United States would commit 60 percent of its global force to such a conflict.[28] With this handicap, the American advantage decreases. For submarines, in particular, the Chinese would have a 1.8 to 1 advantage, a 1.4 to 1 advantage in total tactical fighter aircraft, a 2.3 to 1 advantage in bombers, and a 1.9 to 1 advantage in total personnel. Thus, the United States finds itself at a quantitative disadvantage to China, but not a historically large one. For the world wars, the U.S. military needed to grow four to eight times just to achieve parity with the other powers. Furthermore, this tallying gives no credit for qualitative differences in materiel or for China's requirement to maintain a lengthy land border.

Like GDP, the trends are important; if China were to significantly outpace the United States in military production, it could achieve world war–level numerical superiority in a few decades. Like GDP, military production is possible to obfuscate, but it gives a rough idea of projection capability. Based on inventory changes, China has produced roughly 3 submarines, up to 2 destroyers, and 30 to 40 combat aircraft each year over the past several years.[29] It has focused on modernizing, however, rather than expanding its force, building its own fifth-generation fighters, aircraft carriers, and cruisers rather than expanding capacity.[30] At the same time, growth in Chinese military spending has slowed. After decades of

Maginot Line fortification Ouvrage Michelsberg formed part of Fortified Sector of Boulay and fortified region of Metz, photographed June 10, 2006 (© Pascal Dihé)

double-digit increases, recent years' growth has been 7 percent to 8 percent, only slightly faster than China's GDP growth.[31] With wide skepticism over the Chinese official budget figures, outside experts estimate its 2017 military spending to be between $180 and $216 billion, less than 2 percent of GDP.[32] While a few years ago projections of Chinese military spending had it passing America's by 2030, now that seems unlikely.[33] To do so, China would have to double its military's share of GDP, at a time when China has many other pressing needs.

Meanwhile, current U.S. trends are similar. The Navy seeks to increase from 287 ships to 355 by mid-century.[34] Lockheed Martin built 131 F-35s in 2019.[35] The Air Force intends to buy some 1,763 F-35s in total through 2044, in addition to Navy and Marine Corps purchases.[36] The Air Force is also pursuing the B-21 bomber, expecting to field it in the 2020s and acquire at least 100.[37]

Even assuming a one-for-one drawdown in legacy aircraft, these purchases will keep pace with current Chinese production rates.

Additionally, annual military spending fails to account for accumulated advantage. Even if China spent more on its military annually than did the United States, the incumbent would still benefit from its head start in research and development. Copying technology to catch up is relatively easy, but taking the lead is much harder. Of course, China could ramp up production of known technology in the meantime, but probably not in secret. With its initial advantage, the United States can afford to wait and see.

Based on current military capacity and current trends in production, the United States is not likely to have to mobilize to catch up to China for the foreseeable future. This is not to say the United States is already postured to prevail in a major sustained war with China. The current

military industrial base would certainly need to expand, but starting conditions alone would not drive mobilization the way they did in the world wars. Barring major changes in the force balance, a war should not require industrial catching up at a scale to drive widespread conversion of the civilian economy.

Sustaining a Major War

Even without playing catch-up, a sustained major war could still stress military production to replace combat losses or as part of a strategy to overcome the adversary with quantity. With sufficiently high rates, this could require mobilization. The expected loss rates in a war with China, however, should be more modest. Replacing losses might require a surge of existing capacity, but again not a massive expansion into the civilian economy.

The RAND study estimates potential losses in a Sino-American war based

Table 2. Losses and Production

	2018 Inventory	60% to PAC	Best-Case Loss Rate (5%/year)	Worst-Case Loss Rate (15%/year)	Estimated Production Rate (year)	Estimated Unit Cost (2018$B)	Effective Replacement Rate (%)	Factor to Cover Worst Case	Factor to Cover Double Worst Case
Submarines	54	32	1.6	4.9	3	3.1	9	1.6	3.2
Aircraft Carriers	11	7	0.3	1	0.3	13	4	4	7.9
Large Surface Combatants	87	52	2.6	7.8	3.1	2.1	6	2.5	5
Bombers	139	83	4.2	12.5	0	N/A	N/A	N/A	N/A
Fighters (including Navy)	2,012	1,207	60.4	181.1	217	0.09	18	Exceeds	1.7

Sources: "Chapter Three: North America," *The Military Balance*," 118, no. 1 (2018), 46–63; *An Analysis of the Navy's Fiscal Year 2019 Shipbuilding Plan* (Washington, DC: Congressional Budget Office [CBO], October 2018), 22, available at <www.cbo.gov/publication/54564>; Julia Bergman, "U.S. Navy Gearing Up for Boost in Submarine Production," *Navy Times*, April 23, 2018, available at <www.navytimes.com/news/your-navy/2018/04/23/us-navy-gearing-up-for-boost-in-submarine-production/>; Aircraft carriers: *An Analysis of the Navy's Fiscal Year 2019 Shipbuilding Plan*, 17–18; For large surface combatants, see *An Analysis of the Navy's Fiscal Year 2019 Shipbuilding Plan*, 22–24. Unit cost numbers average the CBO estimates of the upgraded DDG-51 Flight III destroyer and a future large surface combatant. Production rates for bombers are too hypothetical to include, although the Air Force plans to buy at least 100 B-21s, fielding in the mid-2020s. See Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Program Acquisition Cost by Weapon System* (Washington, DC: Department of Defense, February 2020), 1–18. For fighter production rates, see Mike Stone, "Lockheed Martin Reaches 2018 F-35 Delivery Target of 91 Jets," Reuters, December 20, 2018, available at <www.reuters.com/article/us-lockheed-f35/lockheed-martin-reaches-2018-f-35-delivery-target-of-91-jets-idUSKCN1OJ2J9>; "F/A-18 Hornet Production," *Global Security*, available at <www.globalsecurity.org/military/systems/aircraft/f-18-production.htm>; "Chapter Three: North America," 63. Estimated F-35 cost of $100 million per aircraft (for Air Force and Navy variants) and fourth-generation aircraft at $75 million per aircraft are based on *The Cost of Replacing Today's Air Force Fleet* (Washington, DC: CBO, December 2018), 7; Daniel Cebul, "New F-16s Are Headed to Bahrain," *Defense News*, June 25, 2018, available at <www.defensenews.com/air/2018/06/25/new-f-16s-are-headed-to-bahrain/>; Valerie Insinna, "Lawmakers Stand Ready to Protect F-35 from F-15X Budget Threats," *Defense News*, February 27, 2019, available at <www.defensenews.com/digital-show-dailies/air-warfare-symposium/2019/02/27/congressional-supporters-stand-ready-to-protect-f-35-from-f-15x-budget-threats/>.

on projected capabilities in 2025. After "significant" losses in the first days of the conflict (roughly 15 percent of committed American forces), casualties become "heavy" by the end of the first year of fighting, adding another 5 to 15 percent.[38] The study stops after a year, but this linear, steady-state loss rate would likely continue,[39] and a linear rate is expected for sea and air combat.[40] Notably, the study projects heavier Chinese losses, based on the relative quality of equipment, meaning the United States would gain in relative quantity during the conflict.

Over a long war, military production would, at a minimum, need to replace this sustained loss rate, which then gives a low estimate of wartime production. Since there is no upper bound for the production rate assuming a desire to outproduce the enemy, this article arbitrarily targets 30 percent of the committed force per year, doubling RAND's worst case loss rate. This padding offsets adding training equipment, replacing initial losses, and outproducing China to win with mass.

Comparing current production rates to the target indicates required wartime growth. This estimate should

be conservative, since it ignores any peacetime surge capacity. The Navy, for instance, estimates it has 25 percent surge capacity across the board.[41] applies the RAND study's projections to the 2018 U.S. military inventory by major platform with data from recent production or expected production for emerging capabilities, per-unit cost, and effective replacement rates. Finally, it shows the growth required to meet the double worst case loss rate target. The required growth over current production rates shows how much American military production would need to expand for a hypothetical war with China. While significant, it is not massive.

Estimating the intrusion into the civilian economy requires estimating the cost of increased production against GDP. This estimate depends on the expected price of additional equipment at higher levels of demand. Assuming that demand for several times peacetime production would result in doubled prices, table 2 shows the estimated costs of the increased production. Even producing at double the worst case loss rates and doubling the unit price based on surge demand, the total increase in cost would still be less than 1

percent of 2018 U.S. GDP. In that year, the United States spent 3.1 percent of GDP on defense.[42] Even with significant padding, the military share of GDP would grow to only 4 percent (conservatively assuming the extra spending produces no GDP growth). For comparison, during World War I, national security spending rose to 20 percent of the economy, which itself expanded roughly 20 percent from 1914 to 1918.[43] Defense spending peaked at 42 percent of the economy in World War II, alongside 87 percent growth from 1938 to 1944.[44] Although the 4 percent estimate accounts for only some of the increased costs of such a war, the world wars dwarf the magnitude of economic conversion required. The United States spent 4 percent of GDP on defense as recently as 1993, and a far larger portion through the 1970s and 1980s.[45] A war with China would demand a surge by military industry, but not widespread conversion of the civilian economy.

The Right Question: Bets vs. Options
Stepping back from the numbers, it is uncertain how a sustained major conflict with China would play out. Advanced

F-35B Lightning II fighter aircraft assigned to 31st Marine Expeditionary Unit, Marine Medium Tiltrotor 265 (Reinforced), lands on flight deck of USS *America*, South China Sea, April 19, 2020 (U.S. Navy/Vance Hand)

technologies on both sides have never actually faced off in armed conflict. How they might compete against each other is speculation. Defense acquisition choices occur in this uncertainty, pitting present capabilities against future options. At the same time, while a major war with China is the only likely driver of mobilization, it is only one of many scenarios for which the U.S. military must prepare.

This high degree of uncertainty requires an analysis based on risk and options. The key question facing the United States is not how much it could mobilize, but what it needs to face down the uncertainty. Each strategic choice either creates or eliminates options for future decisions, reducing some risks at the cost of increasing others. Business real options are an analogy: A real option creates competitive advantage; maintains flexibility by providing a right rather than an obligation; and

is highly leveraged, offering limited downside and large potential upside.[46] Options are different from "big bets," which may provide an even larger upside, but at the risk of a symmetrically large potential downside.[47] Firms pursue options to avoid the downside risk of a big bet, accepting a reduced but unbounded upside for a known and limited downside. Not all options pay off, but since the downside is limited and the upside is not, the ones that pay off could make up the losses.

National security is hard to value. So are strategic options, but the concept and language of options provide a different way of thinking about choices, especially the value of delaying them in the face of uncertainty. A large part of the uncertainty comes from the interval since the last sustained major war. The use of technology in combat changes quickly. In World War I, tacticians were unprepared for the defensive combination of machine

guns and barbed wire—neither of which were new technologies. Convinced of the durability of this defensive advantage, the interwar French constructed the Maginot Line. World War II, however, saw tanks and airplanes—both of which were used in World War I—smash these defensive measures, a shocking transformation in only 22 years. While the Germans simply drove around the Maginot Line, it remains emblematic of the uncertainty of war, and how quickly its nature can change. Three-quarters of a century later, and with a major war still beyond the horizon, it is hard to predict what technologies might turn the tide. Any concept will be wrong until it clears Carl von Clausewitz's market of combat.[48] The "Maginot Line problem" haunts every military investment, and the greater the commitment to one concept, the greater the potential consequences if it turns out to be wrong.

Sailor tracks contact bearings during Taiwan Strait transit aboard USS *Shiloh*, Taiwan Strait, January 16, 2019 (U.S. Navy/Chanel L. Turner)

The way to combat this uncertainty is by pursuing options in military technology. To start, the United States must ensure its portfolio of military technologies is diversified enough to include whatever emerges as the machine gun of the next war. In this context, the prewar stockpile of a technology is far less important than having developed that technology and considered how to use it. In addition to the Maginot Line, for example, France also had the world's best tank but had not sufficiently considered how to use it.[49] Such diversification, assuming constant budgets, would force smaller stockpiles of each type of equipment. Nevertheless, rather than committing to large buys of any single technology, the United States should ensure that it covers as many technological bases as possible.

More directly, when developing a new technology, the Department of Defense (DOD) could negotiate a production option, buying the ability to increase production when required. Doing so would save the production costs, plus the personnel and sustainment costs, of actually acquiring large quantities of any technology. Additionally, it would increase stability for boom-and-bust contractors, making their capacity investment

decisions easier and therefore cheaper. Contractors could demonstrate that they had worked out the kinks at wartime production rates, but then slow down. That way, surging the equipment for war would mean simply allocating capital to production. For example, the wartime production of large surface combatants assessed earlier requires increasing production five times. If the Navy bought the 13 extra ships per year in peacetime to guarantee the industrial capacity, it would also take on $1.9 billion in annual operations and supply costs, plus the personnel costs of the 9,100 Sailors to crew the ships.[50] In general, since 60 to 80 percent of a system's life cycle cost occurs in sustainment, a production option looks like a good deal even at the full production price.[51] DOD could buy the option, save the sustainment costs, and still keep industry on the hook for the wartime production rate.

In reality, the option should cost less, given the low probability of exercising it. Since a significant indicator of risk for aircraft and shipbuilding contractors is the depth of their order books, DOD could purchase an option that would wait at the end of the line. If the commercial orders dried up, DOD would buy a ship or aircraft to float the contractor over a

dry spell. If a war broke out, the option would entitle DOD to jump to the front of the line. Industry may actually value this demand insurance comparably to the value it assigns to DOD's privilege to jump the line. Contractors may pay for this option, rather than the other way around.

Admittedly, implementing such an approach would require a significant culture shift. Failure of an acquisition program currently means cancelation before it is fielded. Congressional oversight kicks in based on costs and schedule, with programs presumed terminated for certain breaches of cost thresholds.[52] High costs and delays are easy to target as "waste." It is much harder to legislate against a lack of technological ambition, when missing a technological leap becomes clear only in war. Audacious technological advances will run roughshod over budgets and timelines—how does one estimate these things for something never done before? By this way of thinking, *waste* is buying large quantities of equipment that reach obsolescence in the field, rather than expiring as unexecuted options. *Failure* means being late with a technology. We should celebrate options that the military lets go, since letting go means we saved a big bet that would have grown obsolete before it was needed in combat. Thinking of acquisitions as investing in technology and capability options rather than purchasing equipment means diversifying to mitigate surprise (not risk of fielding), containing downside potential while maximizing upside opportunities, and accepting small losses in pursuit of big gains.

Conclusion and Recommendations

Despite the small chance for a sustained major peer war, the existing size of the American military, and the existing production capacity relative to potential demands from such a war, several questions remain for further research:

- To what extent does military production rely on Chinese components or supply systems, which would be at risk during a war with China? DOD is already working on this par-

ticular question.[53] Again, an options approach makes sense. Peacetime acquisition could leverage the cheapest suppliers, but industry should maintain an option on inputs robust to wartime supply restrictions.

- How vulnerable is the industrial base to attack? Adversaries were unable to contest previous U.S. mobilizations, but modern wartime production would be less benign. Industry must produce under attack, at least through space and cyberspace.

- Does the United States have more than one answer to every technological challenge it might face in such a war? Developing options by mastering the technology, production, and tactics should be the priority. Then, only when required and with the latest information (perhaps even from initial combat), DOD could execute options to tailor the fielded force to the nature of the war as it becomes clear. Options rather than big bets mitigate the uncertainty over what form potential wars might take. They are the antidote to the Maginot Line.

At the same time, none of these mobilization issues or concerns should drive an outsized policy change. Chances of a war with China are slim. Chances that such a war would demand widespread conversion of the civilian economy to military production are slimmer still. Other causes of war mobilization are even less likely. Only China appears economically capable of challenging the United States in the kind of sustained major war that might require mobilization. The U.S. military is already comparable in size—and superior in capability—to that of China, even considering global American commitments. The productive capacity of the U.S. military industrial base already comes close to replacing losses in most scenarios for such a war, and expanding this industrial base to outproduce worst case losses requires a much smaller economic conversion than the mobilization efforts in the world wars. Mobilization could easily become a red herring, driving resources away from

more pressing matters, both within the defense budget and within the halls of strategic thought. Even thinking about mobilization generally should focus more on other reasons to harness resources—as COVID-19 has shown—rather than marshaling them for war.

How to mobilize, then, is the wrong question. The right question is how to equip future wartime leaders with the broadest sheaf of technologies, since we cannot predict which will be the right ones, and then train them to make flexible decisions over their use. The nature of the war they could fight might be surprising. Preparing for that uncertainty means developing many options, not placing a few large bets, regardless of how promising a technology appears. This preparation requires a shift in strategic mentality, reframing perspectives on cost, risk, waste, and value. Big bets could turn out far worse. In fact, they could leave strategic choices in someone else's hands altogether. **JFQ**

Notes

[1] Joint Publication 4-05, *Joint Mobilization Planning* (Washington, DC: The Joint Staff, October 23, 2018), ix.

[2] Karen S. Wilhelm, "Mobilizing for War in the 21st Century: An American Perspective" (Ph.D. diss., Georgetown University, March 21, 2012), 17–18, available at <https://repository.library.georgetown.edu/bitstream/handle/10822/557641/Wilhelm_georgetown_0076D_11564.pdf?sequence=1&isAllowed=y>.

[3] Stephen Broadberry and and Mark Harrison, eds., *The Economics of World War I* (Cambridge, UK: Cambridge University Press, 2005), 7.

[4] Mark Harrison, "The Economics of World War II: An Overview," in *The Economics of World War II: Six Great Powers in International Comparison*, ed. Mark Harrison (Cambridge: Cambridge University Press, 1998), 3, 7; updated gross domestic products (GDPs) per capita from Maddison Project Database 2018.

[5] Harrison, "The Economics of World War II," 3, 7; updated GDPs per capita from Maddison Project Database 2018.

[6] Harrison, "The Economics of World War II," 7. This number is based on 1938 GDPs of 1942 Axis and Allied territories, in 1990 dollars, with an older purchasing power parity (PPP) conversion, and taken from Angus Maddison, *Monitoring the World Economy,*

1820–1992 (Paris: OEC Development Centre, 1995).

[7] Harrison, "The Economics of World War II," 7. This number is based on 1938 GDPs of 1942 Axis and Allied territories, in 1990 dollars, with an older PPP conversion, and taken from Maddison, *Monitoring the World Economy, 1820–1992.*

[8] Harrison, "The Economics of World War II," 7. This number is based on 1938 GDPs of 1942 Axis and Allied territories, in 1990 dollars, with an older PPP conversion, and taken from Maddison, *Monitoring the World Economy, 1820–1992.*

[9] Harrison, "The Economics of World War II," 7. This number is based on 1938 GDPs of 1942 Axis and Allied territories, in 1990 dollars, with an older PPP conversion, and taken from Maddison, *Monitoring the World Economy, 1820–1992.*

[10] Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York: Knopf, 2014), 119–126.

[11] *Gross Domestic Product, Fourth Quarter and Annual 2018 (Initial Estimate)* (Hillcrest Heights, MD: U.S. Bureau of Economic Analysis [BEA], February 28, 2019), available at <www.bea.gov/news/2019/initial-gross-domestic-product-4th-quarter-and-annual-2018>.

[12] The World Bank, "GDP, PPP (Current International $)-China," available at <https://data.worldbank.org/indicator/NY.GDP.MKTP.PP.CD?end=2017&locations=CN&start=1990&view=chart>.

[13] *Gross Domestic Product, First Quarter 2020 (Advance Estimate)* (Hillcrest Heights, MD: BEA, April 29, 2020), available at <www.bea.gov/news/2020/gross-domestic-product-1st-quarter-2020-advance-estimate>; National Bureau of Statistics of China, "National Economy Was Generally Stable in 2019 with Main Projected Targets for Development Achieved," January 17, 2020, available at <www.stats.gov.cn/english/PressRelease/202001/t20200117_1723398.html>; Russian Federation Federal State Statistics Service, "Main Economic and Social Indicators," December 2019, available at <https://eng.gks.ru/storage//2020/02-10/FVyjXPxj/December%202019.pdf>.

[14] Conference Board, "Total Economy Database—Data," November 2018, available at <www.conference-board.org/data/economydatabase/index.cfm?id=27762>.

[15] Ibid.

[16] "Editor's Introduction: Western Technology Edge Erodes Further," *The Military Balance* 118, no. 1 (2018), 6.

[17] "China Has Put Missiles on Islands in the South China Sea," *The Economist*, May 10, 2018, available at <www.economist.com/china/2018/05/10/china-has-put-missiles-on-islands-in-the-south-china-sea>; Center for Strategic and International Studies, "Chinese Power Projection Capabilities in the South China Sea," available at <https://amti.csis.org/chinese-power-projection/>.

[18] "China's Might Is Forcing Taiwan to Rethink Its Military," *The Economist*, January 26, 2019, available at <www.economist.com/asia/2019/01/26/chinas-might-is-forcing-taiwan-to-rethink-its-military-strategy>.

[19] David C. Gompert, Astrid Stuth Cevallos, and Cristina L. Garafola, *War with China: Thinking Through the Unthinkable* (Santa Monica: RAND, 2016), 28, available at <www.rand.org/pubs/research_reports/RR1140.html>.

[20] Correlates of War (COW) Project, "National Material Capabilities (v5.0)," last modified February 1, 2017, available at <www.correlatesofwar.org/data-sets/national-material-capabilities>. COW article of record: J. David Singer, Stuart Bremer, and John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820–1965," in *Peace, War, and Numbers*, ed. Bruce Russett (Beverly Hills, CA: Sage, 1972), 1948.

[21] "National Material Capabilities (v5.0)."

[22] Allan R. Millett, Peter Maslowski, and William B. Feis, *For the Common Defense: A Military History of the United States from 1607 to 2012*, 3rd ed. (New York: Free Press, 2012), 297–300.

[23] Martin Gilbert, *The First World War: A Complete History* (New York: Henry Holt, 1994), 341, 378, 400, 419–21, 426, 452; Millett, Maslowski, and Feis, *For the Common Defense*, 317.

[24] COW Project, "National Material Capabilities (v5.0)."

[25] Ibid.

[26] Ibid.

[27] Congressional Budget Office (CBO), *The Budget and Economic Outlook 2019–2029* (Washington, DC: CBO, January 2019), 63, available at <https://www.cbo.gov/system/files/2019-03/54918-Outlook-3.pdf>.

[28] Gompert, Cevallos, and Garafola, *War with China*, 35.

[29] "Chapter Three: North America," *The Military Balance* 118, no. 1 (2018), 46–63; "Chapter Three: North America," *The Military Balance* 117, no. 1 (2017), 45–62; "Chapter Three: North America," *The Military Balance* 116, no. 1 (2016), 27–54; "Chapter Three: North America," *The Military Balance* 115, no. 1 (2015), 29–56; "Chapter Three: North America," *The Military Balance* 114, no. 1 (2014), 31–58; "Chapter Three: North America," *The Military Balance* 113, no. 1 (2013), 49–88; "Chapter Three: North America," *The Military Balance* 112, no. 1 (2012), 39–70; "Chapter Three: North America," *The Military Balance* 111, no. 1 (2011), 41–72; "Chapter One: North America," *The Military Balance* 110, no. 1 (2010), 15–52; "Chapter One: North America," *The Military Balance* 109, no. 1 (2009), 13–52; "Chapter One: North America," *The Military Balance* 108, no. 1 (2008), 135–154; "Chapter Six: Asia," *The Military Balance* 118, no. 1 (2018), 219–314; "Chapter Six: Asia," *The Military Balance* 117,

no. 1 (2017), 237–350; "Chapter Six: Asia," *The Military Balance* 116, no. 1 (2016), 211–306; "Chapter Six: Asia," *The Military Balance* 115, no. 1 (2015), 207–302; "Chapter Six: Asia," *The Military Balance* 114, no. 1 (2014), 201–296; "Chapter Six: Asia," *The Military Balance* 113, no. 1 (2013), 245–352; "Chapter Six: Asia," *The Military Balance* 112, no. 1 (2012), 205–302; "Chapter Six: Asia," *The Military Balance* 111, no. 1 (2011), 195–292; "Chapter Eight: East Asia and Australasia," *The Military Balance* 110, no. 1 (2010), 377–440; "Chapter Eight: East Asia and Australasia," *The Military Balance* 109, no. 1 (2009), 363–424; "Chapter Eight: East Asia and Australasia," *The Military Balance* 108, no. 1 (2008), 359–416.

[30] "Chapter Six: Asia," 2018, 232–233; "Editor's Introduction," 5; Mike Yeo, "China's Military Capabilities Are Booming, but Does Its Defense Industry Mirror That Trend?" *Defense News*, August 14, 2018, available at <www.defensenews.com/top-100/2018/08/14/chinas-military-capabilities-are-booming-but-does-its-defense-industry-mirror-that-trend/>.

[31] Center for Strategic and International Studies, "What Does China Really Spend on Its Military?" *ChinaPower*, available at <https://chinapower.csis.org/military-spending/>.

[32] Ibid.

[33] "Chapter Six: Asia," 2013, 256.

[34] *Report to Congress on the Annual Long-Range Plan for Construction of Naval Vessels for Fiscal Year 2019* (Washington, DC: Office of the Chief of Naval Operations, February 2018), available at <www.secnav.navy.mil/fmc/fmb/Documents/19pres/LONGRANGE_SHIP_PLAN.pdf>; "Fleet Size," *U.S. Naval Vessel Register*, available at <www.nvr.navy.mil/NVR-SHIPS/FLEETSIZE.HTML>.

[35] "Lockheed Martin Hits 2019 F-35 Delivery Target of 131 Jets," Reuters, December 30, 2019, available at <www.reuters.com/article/us-lockheed-f35/lockheed-martin-hits-2019-f-35-delivery-target-of-131-jets-idUSKBN1YY1D3>.

[36] CBO, *The Cost of Replacing Today's Air Force Fleet* (Washington, DC: CBO, December 11, 2018), 7, available at <www.cbo.gov/publication/54657>.

[37] *Program Acquisition Cost by Weapon System* (Washington, DC: Office of the Under Secretary of Defense [Comptroller]/Chief Financial Officer, February 2018), 1–18, available at <https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/FY2019_Weapons.pdf>.

[38] Gompert, Cevallos, and Garafola, *War with China*, 21, 35, 37, 40.

[39] Ibid., 21.

[40] For example, the indirect fire Lanchester equations predict linear losses in air and naval combat. See Michael E. O'Hanlon, *The Science of War: Defense Budgeting, Military Technology, Logistic, and Combat Outcomes* (Princeton: Princeton University Press, 2009), 70–71.

[41] *Report to Congress on the Annual Long-Range Plan for Construction of Naval Vessels for Fiscal Year 2019*.

[42] CBO, *The Budget and Economic Outlook 2019–2029*, 63.

[43] Hugh Rockoff, "Until It's Over, Over There: The U.S. Economy in World War I," in Broadberry and Harrison, *The Economics of World War I*, 312, 334. Calculated as percentage of gross national product.

[44] Hugh Rockoff, "The United States: From Ploughshares to Swords," in *The Economics of World War II*, ed. Mark Harrison (Cambridge, UK: Cambridge University Press, 2009), 88–89.

[45] Ibid., 157.

[46] Hugh Courtney, *20/20 Foresight: Crafting Strategy in an Uncertain World* (Boston: Harvard Business Review Press, 2001), 71.

[47] Ibid., 73.

[48] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 97.

[49] Robert Beckhusen, "France Had a Tank That Could Have Crushed Hitler's Best (But Was Wasted by Bad Generals)," *The National Interest*, February 10, 2017, available at <https://nationalinterest.org/blog/the-buzz/france-had-tank-could-have-crushed-hitlers-best-was-wasted-19410>.

[50] *CBO's Interactive Force Structure Tool* (Washington, DC: CBO, n.d.), available at <www.cbo.gov/publication/54351>. Amounts are in 2017 dollars.

[51] Patrick M. Dallosta and Thomas A. Simcik, "Designing for Supportability," *Defense AT&L: Product Support Issue* (March/April 2012), 34–35.

[52] Moshe Schwartz and Charles V. O'Connor, *The Nunn-McCurdy Act: Background, Analysis, and Issues for Congress*, R41293 (Washington, DC: Congressional Research Service, May 12, 2016).

[53] *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806 (Washington, DC: Department of Defense, September 2018), available at <https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF>.

U.S. Coast Guard Cutter *Bertholf* crewmembers watch from cutter's forecastle as *Bertholf* navigates toward Hong Kong, April 15, 2019 (U.S. Coast Guard/Matthew S. Masaschi)

A Globally Integrated U.S. Coast Guard on a World Stage

By Michael N. St. Jeanos

The Coast Guard is a global force with broad authorities and unique capabilities. . . . We are an instrument of national power at home and abroad, providing solutions across the full spectrum of operations, from security cooperation up to armed conflict.

—Admiral Karl L. Schultz, Commandant, U.S. Coast Guard

U.S. Coast Guard (USCG) domestic competencies can help achieve a globally integrated national security strategy, including counteracting Chinese aggression and influence in the South China Sea as well as Chinese and Russian expansionism into Africa. Global integration transcends the U.S. functional and geographic combatant command construct, allowing for lines of effort across all instruments of national power and domains without geographic constraints. The recent COVID-19 pandemic, for example, underscores our increasingly globalized threat posture—and the corresponding need for globally integrated response capabilities.

Captain Michael N. St. Jeanos, USCGR, currently serves on Active duty at Coast Guard Headquarters in Washington, DC, as Coordinator to the International Maritime Organization for an upcoming member state audit.

Coastguardsman assigned to Pacific Tactical Law Enforcement Teal, Law Enforcement Detachment 108, right, Palauan law enforcement official, and Sailor assigned to USS *Spruance* inspect foreign fishing vessel as part of DOD Oceania Maritime Security Initiative, designed to protect partner-nations' waterways and fisheries, Pacific Ocean, June 3, 2016 (U.S. Navy/Will Gaskill)

Although the USCG is best known for its domestic proficiencies, it also supports Department of Defense (DOD) operations worldwide through its cutter fleet and deployable specialized operations teams. Its nonmilitary capabilities—particularly its vast interagency experience—can help shape the maritime operating environment abroad, offering an asymmetric advantage in locales sensitive to U.S. military presence and where a less threatening and more nuanced footprint might prove advantageous.

In a May 6, 2019, article published in *The Hill*, Admiral Karl L. Schultz, commandant of the USCG, stated that "illicit networks, natural disasters, competing great powers, and hostile adversaries do not respect borders, and in some cases rules-based order." He went on to say that the USCG, as a global force with "broad authorities and unique capabilities," has never been more significant as

an instrument of national power both domestically and abroad.[1] Fully leveraging these Coast Guard competencies can bring a valuable nonmilitary, interagency skill set to the DOD playbook.

Global Integration in Africa and the South China Sea

The concept of global integration is not new. In 1951, Chairman of the Joint Chiefs of Staff (CJCS) General Omar N. Bradley discussed addressing the worldwide strategic situation in a globalized construct through Joint Chiefs of Staff coordination.[2] More than 67 years later, CJCS General Joseph F. Dunford, Jr., addressed Joint Staff personnel at the Pentagon on the need for global integration to maintain a competitive advantage with limited resources. The context of his talk centered on a changing national security dynamic involving a Great Power

competition with China and Russia, which challenges our ability to operate freely across all domains (land, sea, air, and cyberspace) and thereby allows violent extremism and other asymmetric threats to proliferate throughout the global environment. General Dunford confirmed that we will need to adapt to ensure we can project power where and when needed in current and future threat environments.[3]

Historically, we have employed a regional or functional approach to address global strategic threats, operating in a linear and binary framework. This is no longer possible, and we must address current and emerging adversaries by operating transregionally, often without a clear endstate, through application of all instruments of national power and across all domains.[4]

U.S. global integration has lagged in Africa and the South China Sea. In

Africa, the China-Africa partnership employs a regional and transcontinental approach toward infrastructure development, engaging in bilateral agreements such as development of the Tanzanian port of Dar es Salaam.[5] China has also demonstrated strong interest in leveraging Africa's rich mineral resources while opening trading markets and accessing naval ports on the continent. African signatory nations to China's Belt and Road Initiative gain Chinese development and investment in return for this increased access; however, predatory lending practices have created a patron-client relationship from which these nations will not be able to easily extricate themselves.[6] As China has made great strides in securing port access in key developing areas in Africa and moves aggressively to expand its exclusive economic zone and exert naval dominance in the South China Sea, the United States has not been able to fully contain or counter Chinese efforts.[7]

Russia is also exerting influence in underdeveloped nations, particularly those on the resource-abundant African continent. Though many African countries are mineral and hydrocarbon rich, their populaces have failed to realize the benefit of these resources because of corruption and governmental ineptitude; the results are a lack of economic opportunities and a large and disenfranchised youth population, both of which have led to the rise of violent extremist organizations. In his 2019 testimony before the Senate Armed Services Committee, General Thomas Waldhauser, USMC, commander of U.S. Africa Command, discussed Russia's increased influence and militaristic approach in Africa within the context of the U.S.-Africa Command Strategic Approach. General Waldhauser indicated countering this threat will require all instruments of national power in a whole-of-government approach, including strengthening partner capabilities.[8]

U.S. Africa Command does not have robust dedicated resources, though, and has relied on outside support. The U.S. National Guard's State Partnership Program, for example, has proved itself one of U.S. Africa Command's most valuable endeavors. The program,

pairing 14 African nations with 11 U.S. states and the District of Columbia, creates ongoing relationships with African partners for building and improving peacekeeping capacity, disaster management competency, and partner readiness. It has the potential to expand to several more African nations that have requested partnerships, and such growth offers the USCG an opportunity to engage from a maritime interagency perspective.

In 2018, U.S. Naval Forces Europe-Africa continued an annual exercise series with exercises Phoenix Express, Cutlass Express, and Obangame Express to build maritime capabilities of African partner nations, marking the first time in almost 30 years that Somalia participated in a security event outside its borders. In 2018, U.S. Naval Forces Europe-Africa conducted Operation *Junction Rain* as part of the African Maritime Law Enforcement Partnership Program, partnering USCG personnel with Cape Verdeans and Senegalese to counter illegal activities. Capacity-building through U.S.-facilitated exercises, conferences, and operations has offered a strong return on investment.[9]

Fully Leveraging the USCG Globally

Although the United States has made some progress through these partnerships, more can be done to counter and contain Chinese and Russian efforts. In addition to USCG support for DOD through cutters and expeditionary specialized forces, Coast Guard nonmilitary competencies such as fisheries enforcement, marine safety operations, and disaster response could be employed asymmetrically to counteract Chinese aggression in the South China Sea and Chinese and Russian influence in Africa.

Daniel Ward, in a 2017 *Military Review* article, assesses the USCG as a highly valuable but underutilized counterterrorism and counterinsurgency asset due to its dual law enforcement and military roles. He proposes enhanced USCG engagement with DOD for these types of operations, though perception of the Coast Guard in a more nonmilitary posture often hampers its inclusion. The author makes a strong case that the

USCG is, in fact, ideal to be employed for lower intensity conflict. Ward concludes that the USCG's "wealth of capabilities" directly linked to stability operations—particularly those within the civil affairs arena with a focus on maritime, coastal, and riverine environments—provides skill sets not found elsewhere within DOD or the U.S. Government.[10]

Furthering this theme, Rear Admiral David Callahan, USCG, in testimony before the House Armed Services Military Personnel Subcommittee in 2011 concerning USCG Reserve integration with DOD, discussed not only the use of deployable Coast Guard Port Security Units but also the *Deepwater Horizon* oil spill response and the strong interagency skills the USCG Reserve displayed during that event.[11]

The USCG is currently engaged internationally outside of traditional DOD and security-related roles. The Arctic is perhaps one of the most visible examples, with polar icebreakers and membership in an Arctic Council composed of the United States, Canada, Denmark, Finland, Iceland, Norway, Sweden, and the Russian Federation.[12] This resource-rich environment is somewhat atypical, as it lacks an appreciable population and clear ownership under international maritime law. It is an outlier. And yet the specter of global warming opening this once impassible maritime trade route will entail manifest changes in USCG engagement. The Coast Guard is already moving to recapitalize its polar icebreaking capabilities and increase visibility in this emerging maritime corridor.[13]

In April 2019, the USCG *Bertholf* visited Hong Kong—the first USCG cutter to visit in 17 years. A state-of-the-art 418-foot national security cutter operating under tactical control of the commander, U.S. Navy 7th Fleet, its mission centered on professional exchange and capacity-building with partner nations in addition to directed maritime patrols.[14] In contrast to President Theodore Roosevelt's "Great White Fleet" circumnavigation of 1907, intended to project U.S. naval might, this "White Ship" is taking a more nuanced approach to reshaping the maritime operational environment.[15]

Seychelles coastguardsmen simulate boarding vessel during subject matter expert exchange with U.S. Coast Guard as part of Africa Maritime Law Enforcement Program while in Victoria, Seychelles, September 24, 2019 (U.S. Coast Guard/Augustus Manzi)

Asymmetric Application of Fisheries Enforcement

Global integration in fisheries enforcement provides an excellent example of the USCG partnering to help shape the maritime operating environment in a subtle and less threatening manner than might be possible by the other Armed Forces—and although the primary goal lies in resource protection, fisheries enforcement also offers a mechanism to support U.S. strategic policy.

Jay Caputo's 2017 U.S. Naval Institute *Proceedings* article, "A Global Fish War Is Coming," predicts a dire situation for the world's fisheries as a result of overharvest. Climate change, bringing increasingly arid conditions to Asia, Africa, and South America, has resulted in reduced crop yields, while fish consumption has increased from an average of 9.9 kilograms per person in the 1960s to 19.7 kilograms in 2013—and demand is projected to grow. Effective fish management will require multinational cooperation to ensure a sustainable food stock for developing, at-risk nations. This food source is particularly critical in South China Sea nations and in Africa as these areas struggle for economic and food security.[16]

Due to limited worldwide resources, the USCG serves as a global fisheries enforcement integrator. The *U.S. Cooperative Strategy for 21st Century Sea Power* partners the USCG with the Navy and Marine Corps to provide an enforcement presence in areas otherwise lacking this deterrence. In West Africa, for example, the USCG deploys law enforcement detachments (LEDs) and host-nation shipriders on Navy ships to conduct fishery-enforcement boardings. In 2015, an LED was deployed on two Senegalese vessels during the Africa Maritime Partnership, run by U.S. Africa Command. A similar program, though limited in scope, places LEDs on Navy ships moving through the Pacific Ocean under the Oceania Maritime Security Initiative.[17]

Vice Admiral Daniel B. Abel, USCG, Deputy Commandant for Operations, testified in September 2018 before the Senate Subcommittee on Oceans, Atmosphere, Fisheries, and the Coast Guard, affirming not only the domestic importance of effective domestic fisheries management and enforcement but also its international implications. He emphasized the need for the Coast Guard to take a leadership role with the Department of State, the National Oceanic and Atmospheric Administration, nongovernmental organizations, industry, and international partners to reduce the illegal, unreported, and unregulated fishing threat. While countering this threat, "we can increase maritime domain awareness on the high seas and more effectively respond to a range of transnational threats, upholding global order in the maritime domain and asserting American influence through presence."[18]

Although USCG fisheries enforcement demonstrates strong international application in partnering with at-risk African and South China Sea nations for resource protection, the value-added of building relationships, gathering intelligence, and helping shape the maritime operating environment could have a positive impact on U.S. national security

interests. And while recent trade wars may have influenced direct cooperation with China in this regard, potential exists to expand U.S. maritime influence with other South China Sea nations through global application of fisheries enforcement as well as other USCG nonmilitary and primarily domestic competencies.

Recommendation Moving Forward

Effectively combating Chinese and Russian expansionism in Africa and the South China Sea requires a globally integrated approach that could benefit from enhanced USCG involvement. The USCG offers a wide range of nonmilitary capabilities typically employed domestically, such as disaster prevention and response, marine safety, and fisheries enforcement. Coupled with the Coast Guard's strong history of interagency and private-sector collaboration, these competencies could be employed to help strengthen relationships with nations subject to Chinese and Russian influence in a less-threatening and more nuanced way than may be possible through other DOD resources alone. This expansion, however, may come at a cost to existing Coast Guard missions, given finite funding and already stretched resources. Balance is required to ensure an acceptable level of risk to existing mission sets, in what is essentially a zero-sum game.

Conclusion

Although the USCG serves as one of the Nation's five forces capable of joint interoperability, its primary role as the maritime operating arm of the Department of Homeland Security. The smallest of the Armed Forces—with approximately 41,000 Active-duty personnel, 8,000 Reservists, 8,000 civilian employees, and 30,000 volunteer auxiliarists—the Coast Guard enjoys a robust set of domestic nonmilitary missions, serving as a maritime law enforcement, regulatory, environmental, and humanitarian agency.

Providing 24/7 maritime first response, from inland navigable waters to the littoral and high seas, the Coast Guard projects presence around the globe in support of U.S. national interests. In addition to its cutter fleet, Tactical Law Enforcement Teams deployed aboard Navy or allied vessels conduct interdiction-based law enforcement operations, including vessel boardings in offshore locales, while deployable small-boat Port Security Units support combatant commander expeditionary requirements.[19]

The USCG develops partnerships at all levels to help ensure unity of effort, routinely interfacing with global maritime organizations and industry to advance U.S. national interests at home and abroad. The force is proud to be "Always Ready," reflected in its motto, *Semper Paratus*.[20]

Effectively mitigating global threats requires a globally integrated approach employing *all instruments* of national power. Containing and countering Chinese expansion and influence in the South China Sea as well as Chinese and Russian influence on the African continent, for example, could be facilitated by leveraging unique, nonmilitary USCG competencies. This asymmetric application would serve the dual purpose of improving host-nation capabilities while also subtly shaping the maritime operational environment in a less provocative manner than might be possible by DOD alone. **JFQ**

Notes

[1] Karl L. Schultz, "Near a 'Tipping Point,' Coast Guard Needs Lasting Change," *The Hill*, May 6, 2019, available at <https://thehill.com/opinion/national-security/442064-nearing-a-tipping-point-coast-guard-needs-lasting-change>.

[2] "Joint Staff History," Joint History Office Web site, available at <www.jcs.mil/About/Joint-Staff-History/>.

[3] Joseph F. Dunford, Jr., "Global Integration: Maintaining a Competitive Advantage," speech delivered at the Pentagon, October 30, 2018, available at <www.jcs.mil/Media/News/News-Display/Article/1681761/global-integration-maintaining-a-competitive-advantage/>.

[4] Chairman of the Joint Chiefs of Staff Instruction 3050.01, *Implementing Global Integration* (Washington, DC: The Joint Staff, December 31, 2018), A-1–C-13.

[5] Clayton H. Vhumbunu, "Enabling African Regional Infrastructure Renaissance Through the China-Africa Partnership: A Trans-Continental Appraisal," *International Journal of China Studies* 7, no. 3 (December 2016).

[6] Thomas D. Waldhauser, *United States Africa Command and United States Southern Command*, Testimony Before the Senate Armed Services Committee, 116th Cong., 1st sess., February 7, 2019, available at <www.armed-services.senate.gov/imo/media/doc/Waldhauser_02-07-19.pdf>.

[7] Ken Bredemeier, "Obama Sternly Warns China about South China Sea Expansion," *Voice of America News*, June 1, 2015, available at <www.voanews.com/east-asia/obama-sternly-warns-china-about-south-china-sea-expansion>.

[8] Waldhauser, *United States Africa Command and United States Southern Command*.

[9] Ibid.

[10] Daniel E. Ward, "An Underutilized Counterinsurgency Asset: The U.S. Coast Guard," *Military Review*, May–June 2017.

[11] David Callahan, *The Reserve Components as an Operational Force: Potential Legislative and Policy Changes*, Testimony Before the House Armed Services Military Personnel Subcommittee, 112th Cong., 1st sess., July 27, 2011.

[12] Melissa Renee Pegna, "U.S. Arctic Policy: The Need to Ratify a Modified UNCLOS and Secure a Military Presence in the Arctic," *Journal of Maritime Law and Commerce* 44, no. 2 (April 2013), 169–194.

[13] The author draws on his knowledge of Coast Guard Arctic operations and future strategies.

[14] "Coast Guard Ship Visits Hong Kong," news release, U.S. Consulate General Hong Kong and Macau, U.S. Department of Homeland Security, April 14, 2019, available at <https://hk.usconsulate.gov/pr-2019041401/>.

[15] Mike McKinley, "Cruise of the Great White Fleet," Naval History and Heritage Command, September 5, 2017, available at <www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/cruise-great-white-fleet-mckinley.html>.

[16] Jay Caputo, "A Global Fish War Is Coming," U.S. Naval Institute *Proceedings* 143, no. 8 (August 2017).

[17] Ibid.

[18] Daniel B. Abel, *Fish Fights: An Examination of Conflicts over Ocean Resources*, Testimony Before the Senate Oceans, Atmosphere, Fisheries, and the Coast Guard Subcommittee, 115th Cong., 2nd sess., September 18, 2018.

[19] U.S. Coast Guard Publication 3-0, *Operations* (Washington, DC: U.S. Coast Guard, February 2012), 1–8.

[20] Ibid.

Aviation electronics technician 3rd class conducts maintenance on aircraft targeting systems in aircraft intermediate maintenance department maintenance shop on USS *Ronald Reagan*, Philippine Sea, July 25, 2020 (U.S. Navy/Jason Tarleton)

Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat

By Josiah Dykstra, Chris Inglis, and Thomas S. Walcott

Dr. Josiah Dykstra is a Technical Fellow in the Cybersecurity Collaboration Center at the National Security Agency. Chris Inglis is the Robert and Mary M. Looker Professor in Cyber Security Studies at the U.S. Naval Academy. Thomas S. Walcott is the Technical Director in the Cyber National Mission Force at U.S. Cyber Command.

Warfare, with a history as old as humanity itself, has been predominantly conducted through the application of physical force to disrupt, degrade, or destroy physical assets. That long history has led to well-developed doctrine and principles for shows of force, deterrence, proportionality, and rules for warfare that rely on predictable and repeatable characteristics of the physical weapons employed. The advent of cyber warfare in the modern era, however, has illustrated that the assumptions used for the employment of kinetic weapons do not necessarily apply to the employment of cyber capabilities. For example, unlike a physical missile or bomb, it is difficult to predict the precise effects, measure the resulting proportionality, or estimate the collateral effects attendant to the use of a computer virus. As we discuss, the differences between kinetic weapons and cyber weapons are discernible, manageable, and have far-reaching implications for strategic military doctrine, planning, and operational employment in both power projection and defense.

In order to wage and win modern conflict, the attributes of kinetic and

cyber weapons must be fully understood singly and in combination. To date, discussion and debate about the attributes of cyber weapons have focused on a few basic characteristics, such as *perishability*—that is, making it difficult to achieve the same precision, let alone confidence, that typically results from the use of kinetic weapons. For military leaders, and the policymakers who determine the purposes and applications of military power, the differences between kinetic and cyber weapons prompt a reevaluation of how these individuals employ weapons and measure their effectiveness, which foundationally relies on a clear articulation of differences and similarities between the kinetic and cyber environments. We propose and describe a strategic framework, though not exhaustive, that could be applied to any instrument of power employed by a nation-state; we then describe distinctions between kinetic and cyber weapons to draw out both differences and strategic implications.

This article compares instruments of offensive kinetic and cyber power across three key areas: weapons characteristics, targeting, and policy/practice.[1] These thematic categories emerged as we identified 18 individual differences between kinetic and cyber weapons. The weapons characteristics category includes differences in the inherent properties of the weapons as well as in the effects they can deliver. The targeting category highlights divergences in how the weapon influences target selection and pursuit. The policy and practice category covers differences in the current environment and maturity of the weapons.

As we unpack these areas, military leaders should keep in mind three framing questions that can help guide the selection and application of any weapon and that apply equally well to kinetic and cyber:

- Is the weapon able to achieve the desired effect within the constraints of time available for planning and execution, the professional skills of the human operators, and materiel resources?

- Is it possible to limit the weapon's effects to those desired with acceptable impact to innocent parties and assets?

- Will the use of the weapon contribute to, or risk undermining, stability, the ability of the employing organization to manage escalation, and/or other desired characteristics of adversary engagement?

The answers to these questions depend, in part, not only on situational factors but also on a firm understanding of weapon nuances. We draw out those details in the following sections.

To frame the discussion, we must consider the weapons' definitions. Unfortunately, the Department of Defense (DOD) does not explicitly define *weapon* in doctrine, though DOD does use the word within other definitions. We start, therefore, with a dictionary definition for *weapon* as "an instrument of any kind used in warfare or in combat to attack and overcome an enemy."[2] Notably, weapons are traditionally employed to create both lethal and nonlethal effects. Joint Publication (JP) 3-12, *Cyberspace Operations*, defines *cyberspace capability* as "a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace."[3] For the purposes of this discussion, we consider a cyberspace capability distinct from (yet predicated on) some mechanism that enables access to the system within which the intended effect will be achieved. JP 3-0, *Joint Operations*, acknowledges that cyberspace attack is one capability that could create nonlethal effects; other examples include electronic attack, military information support operations, and nonlethal weapons. The military action known as *fires*, states JP 3-0, is to "use available weapons and other systems to create a specific effect on a target."[4] Cyberspace attack actions are a form of fires and "create noticeable denial effects (that is, degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains."

In the following sections we introduce and differentiate 18 characteristics

that are grouped as differences in weapons characteristics, targeting, and policy and practice between cyber weapons and their kinetic counterparts. The table summarizes these differences.

Differences in Weapons Characteristics

Many discussions about cyber weapons have focused on the basic attributes of the cyber domain, such as the global interconnected network; the highly fluid interplay of its constituent components of hardware, software, and configuration; and the resulting fragility of access paths needed by cyber operators to reach their intended targets. Contemporary discussions of cyber weapons have also explored their high degree of perishability and rapid obsolescence.[5] These traits are becoming commonly understood today but are alone insufficient to allow for a comparison of cyber and kinetic weapons. The additional differences below can aid tactical and strategic thinking.

Kinetic weapons typically generate access and effect (by *force*) nearly instantaneously, while cyber weapons necessarily separate access and effect into two distinct actions, often divided by a significant expanse of time (in some cases, cyber access is developed weeks or months in advance of the intended effect). In the Joint Operational Access Concept, the phrase *operational access* is defined as "the ability to project military force into an operational area with sufficient freedom of action to accomplish the mission."[6] Kinetic weapons can produce such access for force projection and provide antiaccess and area denial against opposing forces. Cyber weapons typically separate access from effect, and they often require a significant effort to construct access tailored to the given target and its environment. For example, denial-of-service attacks leverage the access provided by a path from the aggressor to functioning networks. Data destruction attacks control access provided by another means, such as remote exploitation or social engineering, but the key to their success remains an access path from the attacker to the intended target. The

Gunner and cannon crewmember, assigned to Chaos Battery, 4th Battalion, 319th Airborne Field Artillery Regiment, 173rd Airborne Brigade, dials in target of M777 Howitzer during live-fire exercise as part of Saber Junction 19, at 7th Army Training Command's Grafenwoehr Training Area, Germany, September 11, 2019 (U.S. Army/Thomas Mort)

implication is that cyber weapons require significant tailoring, prepositioning, and/or bundling with a target-specific, access-creating capability.

Kinetic weapons almost always produce irreversible physical effects, whereas cyber weapons can produce completely reversible effects. Although a small fraction of weapons (for example, rubber bullets) can deliver a quickly recoverable outcome, most are intended to produce permanent or slow-recovery effects. While cyber weapons can produce permanent damage to the physical world—such as in the case of Stuxnet, which caused physical destruction of centrifuges—other cyber effects can be completely reversed by either the attacker or the victim. For example, when a denial-of-service attack stops, the target systems return to normal. Encryption, such as used in ransomware, is also reversible given the correct decryption key. Indeed, ransomware relies on reversibility in order to be effective; demonstration of the capability to deny access and the subject's belief that it can be undone are the predicate to the victim's willingness to pay ransom. Importantly, reversibility can be an asset or limitation of cyber weapons, depending on the objective of their use.[7]

It is difficult to reverse-engineer and reuse kinetic weapons, since they are typically damaged beyond reuse as a condition of their employment. Because cyber weapons are often comprised of easily replicable software, they offer more ability for others to observe, analyze, and reuse the weapon by simply copying the software and replaying the context of its employment. Given the previously described time delay in constructing access and effecting employment of the cyber weapon, many cyber attacks can be observed and copied using playback capabilities of digital systems designed to monitor the flow and storage of data and software, even if it requires the cyber attack to highlight the significance of a recorded session. The result is a high likelihood that the cyber weapon will be copied intact and studied by an adversary, even if the capture itself is after the attack. Some experts have compared this situation to living in a glass house, arguing that the use of cyber for offense necessitates the preparation and deployment of defenses from the adversary repurposing the weapon against the attacker.[8] In the physical world, weapons platforms can be kept at a distance from their target and thereby protected from harm. Ammunition from kinetic weapons is expendable and, once expended, is generally difficult, impossible, or pointless to reconstruct and replay.[9]

Although in the physical world some weapons—including nuclear, biological, and chemical—challenge weaponeers' abilities to precisely constrain the physical impacts when employed, kinetic weapons typically have a quantifiable local effect governed by attributes of the physical world. And while a nuclear device cannot be configured to destroy only the brick buildings in a particular area, it could be configured and employed to constrain its effects to a physical region. Cyber effects, however, may deliver both local and cascading effects, determined through configuration of the weapon, the target, and the domain of cyberspace. Across the relatively brief span of the history of cyber weapons' employment, seemingly localized domain and network hijacking attacks have often affected the global Internet. The Petya attack attributed to Russia in summer 2017 is an excellent case in point. Though generally assessed to be an attack by Russia on government systems operated by Ukraine,[10] the strike quickly spread to nongovernmental systems across Europe—in one case knocking out most of the global information technology system and associated global command and control of the Maersk shipping line, among many other widespread effects felt well outside Ukraine.[11]

Kinetic weapons deliver consistent, fixed effects that correspond with the attributes of the weapon in a world where the physical properties of the target and its environs, such as gravity and air density, are relatively stable. The same cyber weapon could potentially be used for variable effect, depending on the nuances of coding from subtle (so-called spyware) to dramatic (ransomware). Similarly, a fixed kinetic effect means that outcomes cannot be tailored to a target. Cyber weapons are malleable and can be easily changed or tailored with high granularity to produce a custom effect on only a specific device or chip.

Modern military operations require agility and adaptability in plans and crisis response, including the flexibility to scale operations up and down. Scaling the effects from kinetic attacks generally comes from increasing the literal

Table. Differences Between Kinetic and Cyber Weapons

	Kinetic Weapons	Cyber Weapons
Weapon	Generate access	Leverage access
	Difficult to reverse-engineer and repurpose	Use may result in others adopting it too
	Permanent effect	Potentially reversible effects
	Local effect	Possible global effect
	Consistent effect	Variable effect
	Scale with volume	Scale with use
	Fixed effect	Tailorable effect
	Predictable effect and effectiveness	Sensitive to environmental changes
	High barriers for entry	Low barriers for entry
Targeting	One weapon, one target	One weapon, many targets
	Minimal geographic prepositioning	Can be significant prepositioning (system-specific)
	Positive control	Opportunistic
	Coarse targeting	Surgical targeting
Policy and Practice	Significant experience	Little experience
	Unambiguous intent	Potentially ambiguous intent
	Limited value below level of armed conflict	Useful in all levels
	Overtly attributable	Tailorable attribution
	Confident	Mixed confidence

number, or volume of the payload, of weapons deployed. Because ammunition is expendable, one kinetic weapon at the point of delivery impacts one target. And while the number of kinetic payloads delivered in an area can be increased, there is generally a correlation between payload mass, velocity, and kinetic effect. A single cyber weapon could be used against one or many targets simply by coding the weapons effects, thus enabling inherent and impressively responsive scalability. Ransomware is one example of the same cyber weapon reused against many targets. A defensive corollary is that defending against kinetic weapons requires a per-instance cost. Scaling defense for many targets against a cyber weapon, such as with antivirus software, is comparatively more cost effective.[12]

Military planners likewise benefit when given choices across a spectrum of effects. Kinetic weapons offer fixed effects; that is, the effect is predetermined at the time a given weapon is created. Cyber weapons could also be created with a prescribed action or outcome but are likely to offer a tailorable effect at the time of employment. One can easily

imagine that a weapon capable of deleting a specific file could be rapidly and easily tailored to delete any or many other files. A consequence is that more preparation may be necessary to offer equivalent preparedness and confidence in defending against the cyber weapon.

Kinetic weapons can yield predictable outcomes because the relevant variables influencing the outcomes are well understood. The laws of physics and their effect on kinetic weapons have been studied and documented, and environmental changes have highly predictable and quantifiable impacts on the effectiveness of a kinetic weapon. Cyber effects are extremely sensitive to changes in the environment, from subtle changes in the target's software, hardware, or user settings, to dynamic global networking that serves as the connection between attacker and target. Small, potentially unobserved changes to software or networking could significantly impact the effectiveness of a cyber weapon that relies on very specific software settings.

Finally, we note the difference in the accessibility of kinetic and cyber weapons. Today, entry-level cyber weapons are

Marines with Marine Corps Forces Cyberspace Command in operations center at Lasswell Hall aboard Fort Meade, Maryland, February 5, 2020 (U.S. Marine Corps/Jacob Osborne)

increasingly common as a commodity widely shared by aggressors of varying technical capability. The pervasive availability, low cost, and low expertise necessary to operate them mean that cyber weapons could be employed by many state and nonstate actors. Tools that are freely available (for example, the widely available Metasploit) or on the open market (Core Impact) are easily weaponized for cyber attack. For the United States, this situation is both a liability, in effectively arming more adversaries through the increased exposure of U.S. cyber weapons, and a potential opportunity, by raising the cost to adversaries of conducting cyber attacks by forcing them to counter the greater number of platforms that economies of scale allow the United States to bring to bear. In general, large-scale kinetic weapons,

conversely, continue to remain out of reach in cost, expertise, or availability to many adversaries.

Differences in Targeting

The first difference in the targeting category is in the weapon-to-target ratio. At the point of impact, a kinetic weapon is intended for a single target. Although the scope and scale of the target may vary, even kinetic weapons of mass destruction are limited in time and space. Conversely, cyber weapons offer an ability to affect many targets across time and space, in some cases leveraging each target as the launch platform for the next. Cyber weapons are not expended on use unless someone develops an inoculation, such as a patch—and even in that case, the inoculation may not be global.

Another important distinction is the standoff range from the target. Kinetic weapons can be effective with minimal prepositioning relative to the target—this is particularly true for kinetic weapons of long geographic range. Physical geography matters much less in cyberspace, but the complex digital environment often demands significant prepositioning and initial preparation of the battlespace before the cyber weapon can reach the target.

Targeting is affected by the degree of control over the target (the *find and fix* problem) and the weapon (the *finish* problem). Precise targeting and positive control over the selection of targets for delivery of effects are important to achieving military objectives and avoiding collateral damage. Cyber weapons may require a mix of opportunistic and

discriminating targeting. Stuxnet is a case study where the weapon was designed to roam across many systems, infecting those that met the target criteria while bypassing those that did not.[13] This is an example of opportunistic access as opposed to positive control over the systems infected. It further illustrates the difference between access and effect.

Drawing distinctions in the granularity and precision allowed by kinetic or cyber weapons makes it easy to highlight the difference between the coarse targeting and surgical effect of cyber weapons. Stuxnet had a surgical effect against specific targets, coupled with (comparatively) coarse targeting for access. Precise targeting requires good technical design and good intelligence.[14] There are few, if any, kinetic weapons that can operate with coarse access and surgical effect.

Differences in Policy and Practice

Today, the accumulated experience with cyber weapons has not yet achieved the same maturity as that with kinetic weapons. There is a robust wealth of experience in the development, analysis, and use of kinetic weapons; most have evolved slowly over decades or centuries of refinement and application. The Joint Technical Coordinating Group for Munitions Effectiveness, for example, was established in 1964 to provide weapons effectiveness data in joint munitions effectiveness manuals. No such structure exists for cyber weapons. Furthermore, militaries have extensive experience, including training, in employing kinetic weapons. The relatively recent emergence of cyber weapons has not yet had sufficient time to produce the same amount of experience. As a result, hesitance and uncertainty about integrating cyber as a strategic weapon remain.

When weapons are deployed, their use conveys a message to the adversary. The intent behind the use of kinetic weapons is nearly always unambiguous. The escalation of conflict means that both sides understand, on some level, what the other seeks to achieve through the conflict. The use of force is the last resort for modern nations. Cyber weapons, however, can convey ambiguous messaging, either in their intended effect or in their linkage to a particular actor (the attacker) or a discernible campaign. This situation might be preferred if the cyber weapon was an enabler for an integrated kinetic attack; it could be most undesirable if the cyber attack was the main effort in a campaign designed to impose costs and message the adversary.

Cyber weapons offer unique value in all stages of conflict and confrontation, and they can be particularly effective when employed below the level of armed conflict. Continuous global gray zone conflict in cyber exchanges is likely to occur for the foreseeable future.[15] Kinetic weapons, conversely, are by definition not employed outside of armed conflict—this may be the most distinguishing and important difference between kinetic and cyber weapons. In June 2019, the press reported that U.S. Cyber Command (USCYBERCOM) carried out cyber attacks against Iran in response to Iranian aggression.[16] Although the attack was coordinated with plans for kinetic weapons, the cyber option was executed because the United States apparently elected not to exercise kinetic options. This scenario may demonstrate that cyber was a less escalatory, nonkinetic option that still provided a response and message to Iran.

For nation-states, kinetic weapons carry an overt attribution of the instigator. Attribution in cyberspace remains a difficult problem, as tools and infrastructure are easily obfuscated and manipulated.[17] Cyber weapons, therefore, offer customized attribution. Revealing attribution at a time of the attacker's choosing is a powerful capability.

Humans, including leaders and decisionmakers, weigh their choices, in part, according to their confidence in the options available. Modern military leaders have high confidence in kinetic weapons, owing to experience and training. Today, cyber weapons bring mixed confidence in the effects and effectiveness of the weapons. Persistent operational engagement, combined with science and technology in modeling and simulation, will help build the experience necessary to grow confidence in their effectiveness.

Evolution of Cyber Weapons as a Strategic Capability

Comprehensive national security requires the consideration and coordinated use of all instruments of power across every phase of conflict. It is important to highlight that cyber has only recently emerged as a full instrument of power and strategic capability for the United States. This development was possible given a confluence of deliberate thought and exploration, as well as significant milestones in law, policy, and strategy, but much work remains to elevate cyber's maturity to the level long enjoyed by the kinetic realm of warfare. The growing maturity, especially in the area of policy and practice, will continue to shape the future of integrated warfare.

In 2018, the Defense Science Board (DSB) Task Force on Cyber as a Strategic Capability determined that DOD "must move beyond tactical applications for cyber and realize cyber as a strategic capability."[18] The task force was also asked to compare cyber with kinetic capabilities, including unintended consequences and collateral damage. Key conclusions of the DSB's final report were that, regardless of the means employed to generate a given effect, a strategic capability had the following generic attributes:

- The capability can create a discernible, and preferably enduring, effect on a target's materiel, efficiency, and/or will (that is, the adversary respects and is influenced by the capability).
- The capability is sufficiently well developed and mature that it can generate the desired effect within a reasonable time of a stated need (that is, it is responsive to policy and combatant commander needs).
- The capability can be regenerated within a reasonable time (that is, it can support campaigns in addition to one-time [tactical] strikes).

Four milestones over the past 2 years were instrumental in transforming this

Air Force special tactics operators cross field to approach second target building during operability training at Eglin Range, Florida, April 22, 2020 (U.S. Air Force/Rose Gudex)

aspiration to reality. National Security Presidential Memorandum 13, *U.S. Cyber Operations Policy*, provided the necessary policy,[19] the National Defense Authorization Act for fiscal year 2019 provided the statutory basis,[20] and the DOD Cyber Strategy provided the doctrine.[21] Furthermore, USCYBERCOM was elevated to a combatant command, and its present commander, General Paul Nakasone, USA, has begun to employ these newly assigned authorities under the doctrine of persistent engagement.[22] These milestones demonstrate that the United States is willing and able to employ cyber capabilities, albeit in combination with other capabilities, to protect itself in and through cyberspace.

The Future of Integrated Kinetic and Cyber Combat

The ability to win and prevent modern wars brings an urgent need to understand the unique risks and opportunities of integrated kinetic and cyber warfare. Cyber attacks, independent from kinetic action, are increasingly common, supported by nation-states, and undertaken by independent actors. Yet even conventional warfare is beginning to integrate cyber capability—for example, Russia's invasion of Ukraine was preceded by cyber attacks against critical infrastructure. The United States must quickly learn to integrate cyber capabilities to the greatest possible effect.

The differences between kinetic and cyber weapons explored in this article demonstrate that the capabilities are distinct but complementary and potentially multiplicative in impact when applied in combination. Some researchers have hypothesized that integrating the weapons will even present new and expanded options for military power. JP 3-12 appears to support this assertion, stating that "cyberspace attack capabilities, although they can be used in a stand-alone context, are

generally most effective when integrated with other fires."[23] At present, there is insufficient experience to validate that claim other than intuition. Cyber and kinetic weapons can be incredibly powerful on their own and can achieve a desired military outcome independently. If the ideal of military dominance is to avoid armed conflict altogether, cyber capabilities present unique opportunities to produce a wide range of effects.

Nuanced insight about the differences between weapons allows military leaders to more fully integrate kinetic and cyber. Apart, the kinetic and cyber domains may not deter or stop a modern adversary. New options must be made with respect to the differences between the domains. The military is beginning to learn how, where, and when to use cyber weapons. That knowledge will then allow leaders to determine if these domains could be leveraged in a complementary fashion.

Many open questions remain about the integration of kinetic and cyber combat. By presenting an even broader scope of possible effects, hybrid kinetic-cyber weapons systems and operations raise new questions about the practice of warfare. Unmanned systems are an illustrative example of an integrated weapon: cyber control systems with kinetic effects. The kinetic munition on a drone displays the corresponding kinetic characteristics, including a fixed, predictable, and permanent effect. Targeting, policy, and practice likewise seem to correspond with the offensive attributes of kinetic weapons; however, an adversary targeting the drone or its control system could theoretically produce a tailored, variable, reversible, misattributable effect. Unlike a physical attack against the drone, these attributes complicate the ability to prove that an adversary seized control of the unmanned system; this could delay a defensive response. Unmanned systems also raise questions about what constitutes a valid military target: Is it the remote operator? The location of the operator? The carriers of communications between the operator and the drone? The developers of components of the weapons system?

Whether separately or combined, cyber and kinetic weapons are now available as strategic instruments of power and present novel opportunities for pursuing national objectives. Given the short history of cyber warfare, many opportunities remain for future work to deepen the understanding of cyber weapons. As leaders gain experience and expertise with cyber weapons, integrated combat and gray zone options will be strengthened. The differences in kinetic and cyber weapons outlined in this article are a necessary foundation to understand and leverage the unique and integrated qualities of cyber capabilities. **JFQ**

Notes

[1] While we principally focus on offensive (deny, degrade, disrupt, destroy, and manipulate) capabilities throughout this article, cyber and kinetic effects are also successful for defense and deterrence; these are widely discussed in the literature. Cyber deterrence has been the focus of significant academic and governmental research, making it an area where both practice and theory are rapidly evolving. See, for example, Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017), 381–393, available at <www.sciencedirect.com/science/article/pii/S0030438717300431>. See also Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Department of Defense, February 2017), available at <https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf>.

[2] "Weapon," *OED Online*, Oxford University Press, June 2019.

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

[4] JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, October 22, 2018), III-30, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf>.

[5] Christopher A. Bartos, "Cyber Weapons Are Not Created Equal," U.S. Naval Institute *Proceedings* 142/6/1 (2016), 30–33, available at <https://calhoun.nps.edu/handle/10945/49618>.

[6] *Joint Operational Access Concept*, Version 1.0 (Washington, DC: The Joint Staff, January 17, 2012), ii, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joac_2012.pdf>.

[7] See also N.C. Rowe, "Towards Reversible Cyberattacks," in *Proceedings of the 9th European Conference on Information Warfare Security*, ed. Josef Demergis (Thessaloniki, Greece: University of Macedonia, 2010).

[8] Eric Rosenbach, *Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks*, Testimony Before the Senate Foreign Relations Committee, Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, June 12, 2017, available at <https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf>.

[9] It is possible to imagine re-creating a bullet but hard to imagine the benefit of doing so. It is hard to imagine fully re-creating a missile after it has exploded.

[10] "Alert (TA17-181A): Petya Ransomware," U.S. Department of Homeland Security—Cybersecurity and Infrastructure Security Agency, July 1, 2017, available at <https://www.us-cert.gov/ncas/alerts/TA17-181A>.

[11] "Global Ransomware Attack Causes Turmoil," BBC News, June 28, 2017, available at <https://www.bbc.com/news/technology-40416611>.

[12] Two important notes: First, this presumes known weaponry (that is, the parameters are understood and defenses are known). Second, cyber weapons represent the code that produces the effect and are distinct from the access vector that enables the effect; defenses against the full spectrum of possible access vectors can be quite costly and might not scale well.

[13] Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (Arlington, VA: The Langner Group, November 2013), available at <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.

[14] Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3, no. 1 (March 2017), 59–68, available at <https://academic.oup.com/cybersecurity/article/3/1/59/3097802>.

[15] Defense Science Board, *Summer Study on Capabilities for Constrained Military Operations* (Washington, DC: Department of Defense, December 2016), available at <https://dsb.cto.mil/reports/2010s/DSBSS16_CMO.pdf>.

[16] Julian E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran," *New York Times*, June 22, 2019, available at <www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html>.

[17] See Alexander Kott, Norbou Buchler, and Kristin E. Schaefer, "Kinetic and Cyber," in *Cyber Defense and Situational Awareness*, ed. A. Kott, C. Wang, and R.F. Erbacher (New York: Springer International Publishing, 2014), 29–45, available at <https://arxiv.org/pdf/1511.03531.pdf>.

[18] *Task Force on Cyber as a Strategic Capability: Executive Summary* (Washington, DC: Department of Defense, June 2018), available at <https://www.hsdl.org/?abstract&did=813604>.

[19] Joint Hearing to Receive Testimony on the Cyber Operational Readiness of the Department of Defense, Committee on Armed Services, Subcommittee on Cybersecurity, September 26, 2018, available at <https://www.armed-services.senate.gov/imo/media/doc/18-60_09-26-18.pdf>.

[20] H.R. 5515, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," available at <https://www.congress.gov/bill/115th-congress/house-bill/5515/text>.

[21] *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: Department of Defense, 2018), available at <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>.

[22] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019).

[23] JP 3-12, V-19.

James Meredith walks to class at University of Mississippi accompanied by U.S. Marshal James McShane (left) and John Doar of Justice Department, October 1, 1962 (Library of Congress/ *U.S. News & World Report*/Marion S. Trikosko)

Calling Forth the Military
A Brief History of the Insurrection Act

By Michael R. Rouland and Christian E. Fearer

I n the literal sense, the Insurrection Act does not exist. Rather than a singular piece of legislation, it is a broad, overarching concept for a series of acts dating to the 1790s that concern the use of American military forces within the United States.[1] These statutes, later

Michael R. Rouland and Christian E. Fearer are Senior Historians in the Joint History and Research Office.

codified in current Title 10 *U.S. Code* 251–255, serve as the primary rationale for the delegation of authority to the President to use military forces domestically. In the past 50 years, only one President, George H.W. Bush, has used these emergency powers: in the Virgin Islands in 1989 and in Los Angeles in 1992. The 28 years since the Los Angeles riots mark the longest period in American history without a domestic deployment of troops under the act. In

part, local authorities—many armed and equipped to military standards— have proved more capable of handling disturbances and other crises. Additionally, domestic military deployments have proved politically difficult for Presidents whose critics have attacked such actions as gross usurpations of local authority by an overreaching Federal executive.

Our intention in this article is to outline the key historical events and

decisions that frame the discussion of the Insurrection Act, which we will refer to henceforth as the *militia acts*, and the domestic use of military force. Rather than parse legal terms and interpretations, this historical discussion underlines the seminal events, laws, and court decisions that outline the broad Presidential authorities granted by the Constitution and Congress from our republic's earliest days.

Constitution of the United States

Apprehension over the use of military force is rooted in America's inherited political culture, which held a deep distrust of standing armies and their potential for domestic misuse. The founding generation was especially sensitive to this possibility and worked to alleviate such concerns in the Constitution.[2] The framers were in part spurred to action by the revolt of Daniel Shays in western Massachusetts in 1786, an economic and civil rights protest that revealed the weakness of the new central government under the Articles of Confederation. While there was discomfort at the notion of a regular Federal force or a means to draw state militias into Federal service, this revolt proved a serious threat to order and stability. The challenge was to equip the new Federal Government with the means to enforce the law and maintain order without curtailing the citizens' rights or infringing on states.

Delegates to the Constitutional Convention accepted the premise that the national government must possess a coercive emergency power the earlier articles lacked. A common view, espoused by Alexander Hamilton, argued that "the power of regulating the militia and of commanding its services in times of insurrection and invasion are natural incidents to the duties of superintending the common defence, and of watching over the internal peace of the confederacy."[3] The central point of contention in Philadelphia concerning the domestic use of military force was over who would be responsible for invoking it. A standing military was a powerful instrument. To allay concerns, the Constitution did not grant unequivocal or explicit authority to one branch but gave overlapping authorities to the President and Congress to use the military to quell domestic unrest.

The Constitution guaranteed the United States would protect its constituent states "against Invasion; and on Application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence." Article I granted this authority to Congress in two distinct clauses on the use of the militia. Congress was granted the power "to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions" and "provide for organizing, arming, and disciplining, the Militia, and for governing such Part of them as may be employed in the Service of the United States, reserving to the States respectively." At the same time, the President was granted military authority in Article II: "The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States." As commander in chief, the President would lead and direct those forces called forth by Congress. With respect to domestic unrest, Article II charges that the President "shall take Care that the Laws be faithfully executed." Whether this responsibility refers to broad powers of enforcement or "duty of fidelity" remains debated by legal scholars.[4]

Militia Acts of 1792, 1795, and 1807

Understanding the possibility that certain events may require swift action while Congress is in recess, the Second Congress temporarily delegated its authority under the First Militia Clause to the President by passing a statute "for calling forth the Militia" in May 1792.[5] Under this law, Congress granted a President the authority to "call forth such number of the militia of the state or states" closest to the problem—in this case, invasion by a foreign power, conflict with Native Americans, or an insurrection in a given state—judged necessary to repel the threat. This authority did not permit the President to act unilaterally. Rather, permission to call forth the militia was dependent on a request for assistance by either a state's legislature or governor.[6]

While Congress generally supported emergency executive powers to confront invasions and insurrections, Members of the Second Congress remained concerned over the prospect of using the militias to enforce the laws domestically.[7] There were very few Federal officers in the new republic to enforce Federal law, and those few were ill-equipped to compel compliance. Using martial force to that end made many uncomfortable, presenting what more modern critics might call a slippery slope to overreach and abuse. To guard against this possibility, Congress included judicial, legislative, and temporal checks on the President's new emergency powers. Before a President could employ military force to enforce Federal law, an associate justice of the Supreme Court or Federal district judge had to certify that routine enforcement would be insufficient. Furthermore, anticipating that members of state militias might be unwilling to impose order within their own states, the President was granted the power to call forth militia from neighboring states and to keep them in the field up to 30 days after Congress returned to session.[8]

Still, after granting the President these powers, Congress required additional measures to avoid a confrontation with rioters and irascible citizens. Rather than having troops march straight to the place of unrest, the act required the President to issue a notification ordering the unruly body—insurgents, as described in the bill's language—to disperse.[9] With all these precautions and protections, however, Congress was unwilling to permanently cede these powers, including in the bill's final section an expiration by the end of the next Congress.[10]

Two years later, in July 1794, President George Washington relied on this authority when responding to armed farmers protesting the new Federal excise tax in western Pennsylvania during what is known as the Whiskey Rebellion, thereby demonstrating the will of the

Within 1 hour of President Eisenhower's decision on September 24, 1957, Soldiers from 1st Airborne Battle Group, 327th Infantry Regiment, deployed to Little Rock, Arkansas, to escort nine Black high school students into formerly segregated Central High School amid racial protests (U.S. Army)

newly established Federal Government to suppress violent resistance to its laws. After negotiations failed to resolve the dispute, Washington requested certification from a Supreme Court justice that local law enforcement could no longer enforce the law. He then issued a proclamation in August indicating that he would raise a militia and demanded the Pennsylvania insurgents disperse by September 1. Washington, with the governor's support, assembled 13,000 militiamen from Pennsylvania and three other states. As the army marched west, the rebels dispersed.[11] When the army remained in the field as Congress came into session, legislators reauthorized the calling forth of the militia for an additional 3 months. Yet, to allay concerns

over potential abuses by the army, Washington disbanded the federalized force, its purpose achieved. At the time, critics generally praised Washington for his actions against the whiskey rebels and reaffirmed the validity of the Militia Act.[12] Washington demonstrated clear and persuasive deference to both the courts and the legislature in committing armed forces to dispel the largest incident of armed resistance to Federal authority between the Constitution's ratification and the Civil War.

The Third Congress replaced the original statutes in the Calling Forth Act with a new Militia Act in February 1795.[13] While the Second Congress intended the delegation of authority to call forth the militia to be temporary and required the

explicit support of a Federal judge, the Third Congress made the delegation of authority permanent and eliminated three key checks on the President's authority: the antecedent court order, the limits on out-of-state militia, and the time requirements on the notification for dispersal.[14] The President could now act quickly and unilaterally. As amended in 1795, this iteration of the Militia Act provided the foundation for the current law for 10 *U.S. Code*, Section 251.

The next century brought new challenges, prompting new laws. Thirteen years after Washington marched against the whiskey rebels, President Thomas Jefferson sought to use Federal troops—distinct from state militias—to challenge Spanish border incursions along the new

frontier at Natchitoches, Louisiana, and to intercept his former Vice President, Aaron Burr, who was suspected of organizing a filibuster expedition into Mexico.[15] Jefferson himself drafted a new law *authorizing the employment of the land and naval forces of the United States, in cases of insurrections* that was approved by the Ninth Congress in March 1807, one of several bills passed on its last day.[16] This legislation was an important expansion of emergency powers by adding Federal forces to the state militias available to quell insurrections and domestic unrest.

Congress refrained from passing any similar law for the next 50 years, although Federal Soldiers were used domestically for a variety of purposes and almost always in support of state governments that simply required additional forces. Cases included the putting down of slave revolts, enforcing fugitive slave laws, combatting vigilantism, and enforcing Federal laws governing relations with American Indians.

Instrumental Supreme Court Decisions of the 19th Century

While constitutional authority for the use of military force was clearly articulated in Articles I and II, the judiciary likewise weighed in on the subject. In the first half of the 19th century, two Supreme Court cases, *Martin v. Mott* (1827) and *Luther v. Borden* (1849), provided additional context for the statutory discussion of the President's authority to call forth the militia and would validate the President's broad powers derived from the militia acts. In both cases, the courts ultimately deferred to the executive to establish the limits on this authority.

Martin v. Mott adjudicated whether a citizen could be court-martialed for failure to report to the New York militia when the President called it up during the War of 1812. Justice Joseph Story, writing for the court, rejected the argument that the President lacked the authority to call forth individual citizens in their state militias, arguing that such authority came from the 1795 Militia Act. Specifically, Story argued that the

court shared the opinion "that the authority to decide whether the exigency has arisen, belongs exclusively to the President, and that his decision is conclusive upon all other persons." Story continued that the power was confided to the President as commander in chief and whose duty is to "take care that the laws be faithfully executed" and "whose responsibility for an honest discharge of his official obligations is secured by the highest sanctions."[17] Ultimately, the court confirmed a broad and unchallenged authority for the President when acting appropriately in calling forth the militia. Moreover, the court sided with the President over the states in deciding when to call forth the militia.[18]

Luther v. Borden was another early test for the Supreme Court to evaluate the legality of the President's "calling forth of the militia." Writing for the court, Chief Justice Roger B. Taney argued, "It is said that this power in the President is dangerous to liberty, and may be abused. All power may be abused if placed in unworthy hands."[19] The court did not suggest that such power was without a check. "Undoubtedly," Taney wrote, "if the President in exercising this power shall fall into error, or invade the rights of the people of the State, it would be in the power of Congress to apply the proper remedy. But the courts must administer the law as they find it."[20] Scholars have generally agreed that this decision codified the President's emergency powers as well as their basis in the militia acts.[21]

The 1860s and 1870s: Suppression of the Rebellion to the Third Enforcement Act

Immediately after the attack on Fort Sumter and the seizure of other Federal property in the South, President Abraham Lincoln issued a proclamation closely following the formula laid down by the 1795 law, calling on the states for a militia of 75,000 men to oppose combinations too powerful to be suppressed by the ordinary course of judicial proceedings. Attorney General Edward Bates justified the administration's measures by citing

Taney's opinion in *Luther v. Borden*, writing that "the duty to suppress the insurrection, being obvious and imperative, the two acts of Congress, of 1795 and 1807, come to his aid, and furnish the physical force which he needs, to suppress the insurrection and *execute the laws*. Those two acts authorize the president to employ, for that purpose, the Militia, the Army and the Navy."[22]

Lincoln issued further proclamations closing Southern ports, calling for a limited number of volunteers to serve for 3 years, increasing the size of the Regular Army and Navy, and suspending the writ of habeas corpus in certain areas. These actions were a tremendous expansion of the use of armed forces and executive power itself. Yet when the Thirty-Seventh Congress convened on July 4, it ratified Lincoln's actions and passed additional laws that would enable him to mount a full-scale effort to compel the rebellious states' return to the Union.

In particular, in late July 1861, Congress approved *An act to provide for the Suppression of Rebellion against and Resistance to the Laws of the United States.* Grounded in the 1795 Militia Act, this measure expanded the discretion of the President to call forth both the militia and Regular Army to suppress insurrections and execute the laws of the Union. The trend of the multiple versions of the militia acts since 1792 was one of increasing the authority of the President to call forth the militia. (The current language in 10 *U.S. Code*, Sections 252 and 254, remains virtually unchanged since July 1861.) Lincoln secured a definitive expansion of Presidential authority in the first section of the 1861 Militia Act with the addition of the President's ability to call forth the militia to "enforce the faithful execution of the laws of the United States."[23] According to James Randall, author of the most comprehensive legal analysis of Lincoln's actions, "the emergency, as interpreted by the Lincoln administration, was precisely that for which the use of militia had been expressly authorized. To execute the laws, to suppress an insurrection, to put down combinations

too powerful for judicial methods—these were the purposes for which the Government needed troops."[24]

While this 1861 act was drafted with the rebellious states in mind, Lincoln relied on these authorities to suppress disorder within the loyal states during the war as well, most infamously during the 1863 New York City draft riots. Bloodshed in the city's streets, wrought by the military and rioters, caused considerable consternation for the Lincoln administration. His critics in Congress, as well as in the South, argued that the deployment of troops to suppress the riots was further evidence that the President was a tyrant.

Once more, the Supreme Court would ultimately judge the boundaries of the President's authority in the *Prize Cases* (1863) decision. Justice Robert Cooper Grier wrote on behalf of the court, and this opinion remains a definitive statement of war powers under the laws of the United States. Grier explained that Congress did not need to give the President the authority to act unilaterally in 1861 because congressional authority was already granted in 1795 and 1807. "Whether the President in fulfilling his duties, as Commander-in-chief, in suppressing an insurrection, has met with such armed hostile resistance, and a civil war of such alarming proportions as will compel him to accord to them the character of belligerents, is a question to be decided *by him*," Grier wrote, "and this Court must be governed by the decisions and acts of the political department of the Government to which this power was entrusted. He must determine what degree of force the crisis demands."[25] While confirming the President had considerable powers, the court ultimately deferred to Congress, as that body had established the legal precedent and the broad parameters for the President to call forth the military.

After the war, Federal military forces were garrisoned throughout the South during Reconstruction and were relied on to uphold Federal law in the former Confederate states and check violence perpetrated by the Ku Klux Klan and other white supremacists. In its most

recent modification to the militia acts in 1871, Congress approved *An Act to enforce the Provisions of the Fourteenth Amendment to the Constitution of the United States, and for other Purposes.* This act allowed the President to use the military when domestic violence or an insurrection resulted in the denial of citizenship rights or equal protection conferred to citizens by the new Fourteenth Amendment.[26] And although the 1871 Militia Act specifically targeted violence instigated by the Klan, the delegation of authority was broader than the 1861 version, including not only calling forth the militia and Regular Army but also "other means" to enforce the protections granted by the Fourteenth Amendment. This act is also noteworthy in that the President did not require a request or approval from the state government to call forth the military when Federal laws or civil rights were at stake. As updated, this militia act provided the foundation for the current law for 10 *U.S. Code*, Section 253.

Critics argued that this latest law blurred distinctions between insurrection and lesser forms of civil unrest. They worried that such provisions allowed the President to deploy forces to combat minor incidents of civil disorder that they argued were state affairs regardless of whether state authorities requested Federal assistance. More than a reflection on the President's evolving authority to deploy the military domestically, the 1871 Militia Act reflected changes in the ways the courts and Congress were applying the Constitution as a check against abuses by states after the Civil War. Taking advantage of the broad affirmation of the President's authority to quell unrest and enforce Federal law, Presidents began to call on the military for a variety of reasons beyond Reconstruction. The end of the 19th century was a tumultuous period, one in which a rapidly industrializing America witnessed widespread social strife. Presidents increasingly called on military forces to protect property, aid in enforcing Federal laws, and protect victimized minorities from mob violence.

The Posse Comitatus Act of 1878 and Domestic Disputes into the Early 20th Century

The 1861 and 1871 revisions of the 1795 Militia Act granted the President broad statutory discretion to use state militias or the Regular Army to confront domestic unrest. Congress and the courts were both complicit in this expansion of executive power. With the Posse Comitatus Act of 1878, Congress introduced a new check on the use of the military to enforce civil law. More recently, this has been viewed by military leaders as an important check on the military's role in domestic law enforcement, but it was not viewed in this manner by Presidents at its inception.

Congress intended the Posse Comitatus Act to correct a specific set of military law enforcement issues emerging from an opinion expressed by Attorney General Caleb Cushing in May 1854, during Franklin Pierce's administration. At the time, Cushing argued that under Section 27 of the Judiciary Act of 1789, U.S. marshals could raise a posse comitatus of men regardless of their

occupation, whether civilian or not, and including the military of all denominations, militia, soldiers, marines, all of whom are alike bound to obey the commands of a sheriff or marshal. The fact that they are organized as military bodies, under the immediate command of their own officers, does not in any way affect their legal character. They are still the posse comitatus.[27]

Twenty-four years later, President Rutherford B. Hayes's attorney general was advancing similar arguments, and Congress responded with a legal remedy in the Posse Comitatus Act.[28] This law, driven by Southern Members of Congress responding to the widespread and unconstrained use of Regular Army forces during Reconstruction, specifically stated that

it shall not be lawful to employ any part of the Army of the United States as a posse comitatus, or otherwise, for the purpose of executing the laws, except in such cases

The Evacuation of Fort Sumter, albumen silver print from glass negative, J.M. Osborn, April 1861 (Metropolitan Museum of Art/Gilman Collection)

and under such circumstances as such employment of said force may be expressly authorized by the Constitution or by act of Congress.[29]

Ultimately, the Posse Comitatus Act confirmed that only Congress or the President could authorize the military to execute or enforce the law.

By century's end, despite the multiple and flexible legislative options for the President to use Federal forces in aiding civil authorities, state and Federal authorities often had difficulty in determining which statutes applied to their unusual circumstances of domestic unrest. In numerous cases, Presidents simply dispatched units to the proximity of a disturbance without seeking a specific state request or statutory justification. The threat of intervention or mere

presence of the Regular Army was often enough to restore order without using the formal process for direct Federal military intervention. After the first major Regular Army intervention in a labor dispute during the Great Railroad Strike of 1877, Presidents felt increasingly secure deploying military forces—both state and Federal—to confront domestic unrest.

A critical test was the Pullman Strike in May and June 1894, which involved 250,000 striking rail workers in 27 states shutting down most of the railways west of Detroit, Michigan. When President Grover Cleveland demanded strikers stop interfering with trains carrying mail, they refused, and Cleveland sent in thousands of marshals and 12,000 Soldiers.[30] The following year, organizer Eugene V. Debs challenged the Federal Government's authority to intervene and in so doing

brought the courts to adjudicate the use of the military as well.

In the *In re Debs* decision of 1895, the Supreme Court confirmed unanimously that the government had broad powers under the Sherman Antitrust Law to protect the mail and interstate commerce. The court sustained the President's use of the military and explained that "the strong arm of the national government may be put forth to brush away all obstructions to the freedom of interstate commerce or to the transportation of the mails. If the emergency arises, the army of the Nation, and all its militia, are at the service of the Nation to compel obedience to its laws."[31] As the Posse Comitatus Act suggested, there are limits on the domestic use of the military, but "insurrection, domestic violence, unlawful combinations, or conspiracies" provided the President

essentially unfettered authority to respond in preservation of the law.

For instance, in 1903, President Theodore Roosevelt sent military forces to pacify labor disputes in Arizona and Colorado; 4 years later, he acted similarly in Nevada. In the summer of 1919, President Woodrow Wilson suppressed race riots in Washington, DC; Omaha, Nebraska; Elaine, Arkansas; and Lexington, Kentucky.[32] Wilson also quelled labor unrest with Federal forces in Butte, Montana; Seattle, Washington; Gary, Indiana; Knoxville, Tennessee; and Denver, Colorado, in 1919 and 1920.[33] And the National Guard and Regular Army took part in West Virginia's mine wars in 1920–1921. The military proved largely effective, and it consequentially became a Presidential tool of first (rather than last) resort in these complex cases.

Effective as it may have been, the use of the military in this capacity continued to provoke criticism. While public attitudes toward strikers and protestors varied, reports of Federal military forces using brutal—and at times lethal—force were met with stern criticism within Congress and among the people, especially among those groups against whom the force was directed, whether they were labor organizations, citizens of a particular region, or some broader class. Meanwhile, in January 1903, Congress sought "to promote the efficiency of the militia," thereby redefining the militia and establishing tighter Federal control of the National Guard, which had by this time developed a reputation for harsh anti-labor attitudes and practices.[34] The Regular Army, on the other hand, was regarded as inherently nonpartisan, more reliable, and generally more efficient.

The Apogee and Abandonment of the Militia Acts in the 20th Century

The decades following World War II saw significant unrest throughout the United States, prompted by issues of race and an unpopular war in Vietnam. Presidents continued to deploy military forces to compel adherence to Federal law and to support local authorities in restoring order. The former consis-

tently proved controversial. However, before the civil rights era began in earnest, the Supreme Court weighed in for the first time to check the President's seemingly unfettered militia act authorities in *Youngstown Sheet & Tube Co. v. Sawyer* (1952).

In April 1952, President Harry S. Truman issued an executive order directing Secretary of Commerce Charles W. Sawyer to seize most of the Nation's steel mills and avert a potential strike that could undermine the national defense and military operations in the Korean War, citing his authorities in the Constitution and laws of the United States. This action was immediately challenged in the courts. In *Youngstown Sheet & Tube Co. v. Sawyer*, the Supreme Court addressed the power of the President to act without express constitutional or statuary authority. By a vote of six to three, the court resolved that the President acted unconstitutionally.[35]

Justice Hugo L. Black wrote the majority opinion, but six other justices also wrote opinions, offering insights into the constitutional authorities of the President on military matters. Black's opinion stated that "the President's power, if any, to issue the order must stem either from an act of Congress or from the Constitution itself."[36] Truman had contended that "presidential power should be implied from the aggregate of his powers under the Constitution" and that based on provisions in Article II which state that "he shall take Care that the Laws be faithfully executed" and that he "shall be Commander in Chief of the Army and Navy of the United States." Black wrote that Truman's commander-in-chief argument "cannot properly be sustained. . . . The Government attempts to do so by citing a number of cases upholding broad powers in military commanders engaged in day-to-day fighting in a theater of war."[37] Commanding in a theater of war was far different from "commanding" private businesses within the United States.

Justice William O. Douglas noted in his concurring opinion that "our history and tradition rebel at the thought that the grant of military power carries with

it authority over civilian affairs."[38] Justice Robert H. Jackson concluded in his concurrence, "Congress . . . authorized the President to use the army to enforce certain civil rights. On the other hand, Congress has forbidden him to use the army for the purpose executing general laws except when *expressly* authorized by the Constitution or Act of Congress."[39] He observed that "when the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain."[40] Finally, reflecting on the many military emergencies of the past century, Jackson cautioned that our forefathers "knew what emergencies were, knew the pressures they engender for authoritative action, knew, too, how they afford a ready pretext for usurpation. We may also suspect that they suspected that emergency powers would tend to kindle emergencies."[41]

Civil rights legislation brought new challenges to Federal authority akin to those encountered in the wake of the Fourteenth Amendment. The passage of the 1957 Civil Rights Act and the Supreme Court's earlier decision in *Brown v. Board of Education* (1954), mandating school desegregation, prompted a harsh backlash across the South. In 1957, Arkansas's governor vowed to resist desegregation and used his state's police and National Guard to prevent black students from accessing Little Rock Central High School. President Dwight D. Eisenhower believed that a failure to act by the Federal Government would be tantamount to acquiescence to anarchy. He argued that the governor's actions were a direct obstruction of Federal law, signed a proclamation commanding Arkansas police to disperse, federalized portions of the state's guard, and sent five rifle companies of the 101st Airborne Division to the state capital to enforce the court order. Segregationist Arkansans were irate. Rather than desegregate at the point of the bayonet, the governor closed the state's high schools for the following year.

A more dramatic episode unfolded 5 years later in Oxford, Mississippi, when
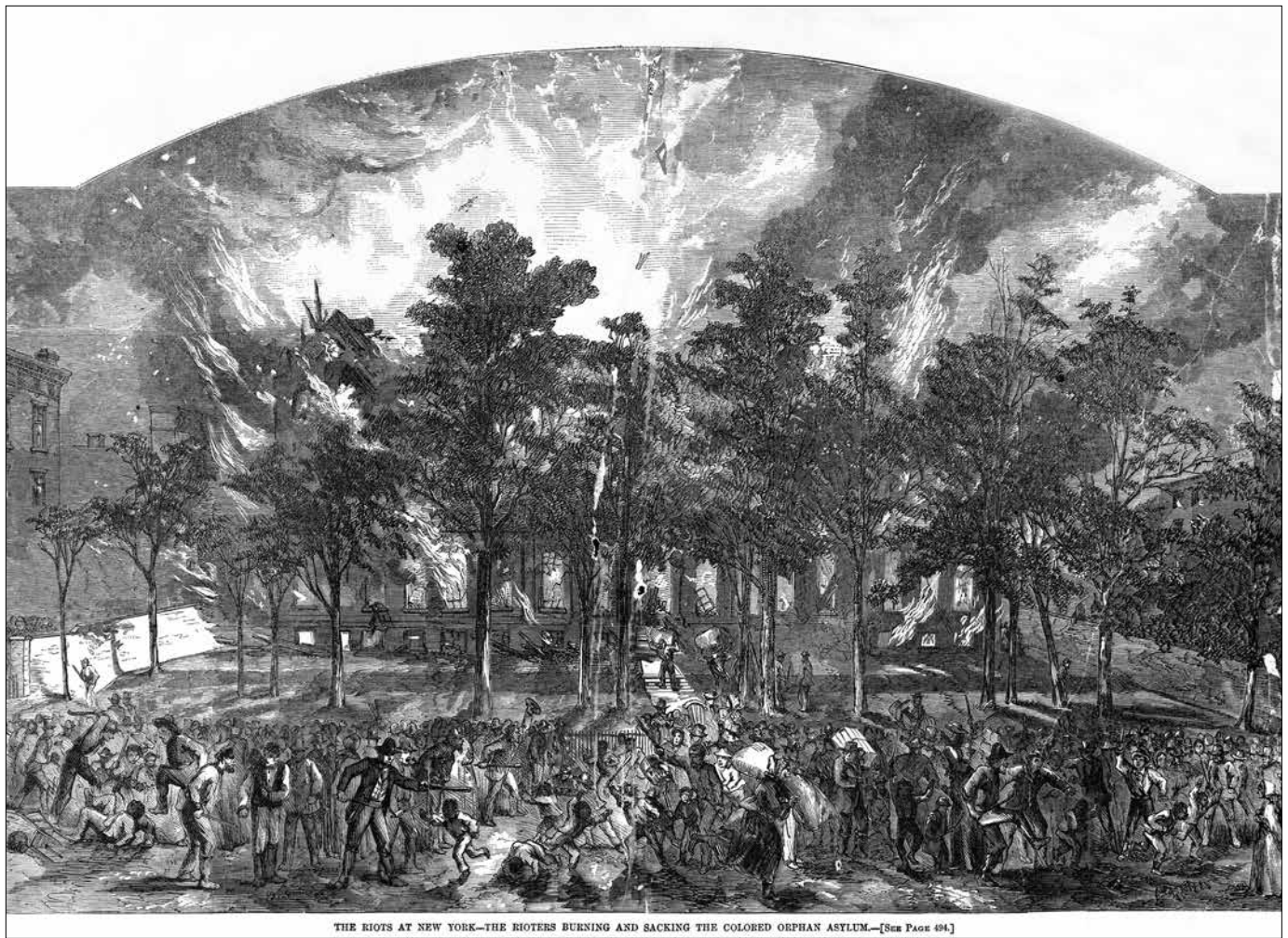
The Riots at New York—The Rioters Burning and Sacking the Colored Orphan Asylum, 5th Avenue and 46th Street, New York City draft riot in 1863, wood engraving in *Harper's Pictorial History of the Civil War*, ca. 1866–1868 (Library of Congress)

a black student sought to enroll at the University of Mississippi. The state's governor vowed to defy a court order that the student be allowed to matriculate, prompting President John F. Kennedy to utilize U.S. marshals, federalized national guardsmen, and deployed Regular Army soldiers; their combined force numbered nearly 30,000. Segregationists reacted violently in a 2-day riot dubbed the Battle of Oxford, shooting at Army convoys and attacking troops and marshals. Federal forces remained in Oxford for 9 months. As in Arkansas, local citizens and their political leaders argued that Federal troops were the tools of an abusive, overreaching Federal Government intent on forcing its will on a matter of local concern.

The clash in Oxford was one of many instances of unrest during the 1960s, a decade of social disruption prompted

by deep-rooted racial antagonisms, the civil rights movement, and opposition to the Vietnam War. Federal troops were deployed on a number of occasions to help local authorities quell unrest and restore order. For example, Federal forces were sent to the Nation's capital for the March on Washington for Jobs and Freedom in 1963 in the event protests turned violent and to Detroit in 1967 to help local authorities subdue a violent race riot. Antiwar demonstrations gathered momentum in October 1967 when a major rally in Washington turned toward the Pentagon and was met by military police, Federal marshals, and Active-duty Soldiers. Federal forces were used in that case to maintain order and returned 6 months later to help restore order during the 1968 riots following the assassination of Martin Luther King, Jr. Troops were

likewise deployed to Detroit, Baltimore, and Chicago that month after violent riots in those cities. Eventually, 23,000 Regular Army and 15,600 federalized National Guard Soldiers were collectively used in these responses. In each case, Presidents issued a proclamation ordering dispersal forthwith in recognition of the legal obligations established by the 1795 Militia Act.

Responding 20 years later to "conditions of domestic violence and disorder" that resulted from Hurricane Hugo, President George H.W. Bush deployed 1,200 military police and Federal marshals to St. Croix in the U.S. Virgin Islands in September 1989, when local police could not contain an outbreak of violence. The most recent use of the militia acts occurred in May 1992 when Bush deployed troops to restore order

Washington Reviewing the Western Army at Fort Cumberland, Maryland [before their march to suppress the Whiskey Rebellion in western Pennsylvania], oil painting, attributed to Frederick Kemmelmeyer, after 1795 (Metropolitan Museum of Art)

in Los Angeles when rioting broke out after white police officers were acquitted of using excessive force against Rodney King, an unarmed black man. Nearly 10,000 California National Guardsmen mobilized. When they could not quell unrest, California's governor requested Federal assistance. Bush then deployed 2,000 Soldiers from the 7th Infantry Division and 1,500 Marines from the 1st Marine Division to help local and state authorities. In both cases, governors requested Federal support.

No President since then has deployed Federal forces in the United States to enforce Federal law and restore civil order under the terms of calling forth the military. Political considerations have weighed heavily in recent Presidential decisions not to use Federal military forces domestically; the evolution of the all-volunteer force since the 1970s may also play a role. Increasing capabilities of local law enforcement to handle domestic disorders

have accompanied the increasing political opposition to using Federal troops for the same purposes, rendering the Federal Government's involvement unnecessary and perhaps coercive. For the last three decades, Presidents appear to have accepted that calling in Federal forces is a measure to be saved for truly grave crises in which there is no serious dispute over the need for Federal intervention.

Conclusion

Since our nation's founding, Congress has seen fit to support the need for emergency powers for the President to confront "insurrection, domestic violence, unlawful combinations, or conspiracies." There has been no congressional effort to revoke the authority to call forth the militias. Congress instead expanded the President's powers on four occasions. History demonstrates how both Congress and the courts have repeatedly deferred to Presidents.

Importantly, this emergency power is not inherent in the Constitution and thus subject to judicial review and legislative action. Supreme Court cases—especially *Martin v. Mott* (1827), *Luther v. Borden* (1849), and the *Prize Cases* (1863)—affirmed the foundational authority of the militia acts as well as the President's all-encompassing, congressionally delegated authority to act appropriately. *Youngstown Sheet & Tube Co. v. Sawyer* (1952), however, raised the concern that domestic use of the military requires congressional authorization and that a President cannot act with impunity on military matters.

The Civil War had a profound influence on the militia law, and subsequent Presidents called forth the military on more than 125 occasions before World War II to quell violent labor disputes and race riots. The use of Federal military forces provided valuable social stability

Special patrolling train Rock Island Railroad, with Company C, 15th U.S. Infantry, at Blue Island, Illinois, during great railroad strike, 1894 (Foss Etching & Photo Company)

and assured that changes in American institutions were evolutionary and not revolutionary in nature during an era of radical economic and social changes.[42] Again, in the 1950s and 1960s, Presidents called on military forces to maintain order during the movement for and reactions against civil rights. Over the course of a century, military leaders emphasized tactical restraint, military command and control of federal troops, strict adherence to legal guidelines, and discipline that would prove valuable in the effective use of this emergency power. Although no President has exercised these authorities since 1992, it is reasonable to assume a future President could, although Congress would determine the parameters and restrictions for calling forth the military. For its part, the military—Active, Guard, and Reserve—should understand the legal framework that supports the lawful orders of a President. **JFQ**

Notes

[1] The five statutes are the Calling Forth Act of 1792, ch. 28, 1 Militia Act of 1795, ch. 36, 1 Stat. 424 (repealed in part 1861 and c 331-335 [2000]); the Insurrection Act of 1807, ch. 39, 2 Stat. 443 (331-335 [2000]); the Suppression of the Rebellion Act of 1861, version at 10 *U.S. Code* 331-335 [2000]); and specific parts of the Act of 1871, ch. 22, 3-4, 17 Stat. 13, 14-15 (expired in part 18 *U.S. Code* 333).

[2] See Frederick T. Wilson, *Federal Aid in Domestic Disturbances, 1787–1903*, Senate Document 57-209 (2nd sess., 1903); Frederick T. Wilson, *Federal Aid in Domestic Disturbances, 1903–1922*, Senate Document 67-263 (2nd sess., 1922); Frederick Bernays Wiener, "The Militia Clause of the Constitution," *Harvard Law Review* 54, no. 2 (December 1940), 181–220; Richard H. Kohn, *Eagle and Sword: The Federalists and the Creation of the Military Establishment in America, 1783–1802* (New York: Free Press, 1975); Robert W. Coakley, *The Role of Federal Military Forces in Domestic Disorders, 1789–1878* (Washington, DC: U.S. Army Center of Military History, 1988); Henry P. Monaghan, "The Protective Power of the Presidency," *Columbia Law Review* 93, no. 1

(January 1993), 1–74; Clayton D. Laurie and Ronald H. Cole, *The Role of Federal Military Forces in Domestic Disorders, 1877–1945* (Washington, DC: U.S. Army Center of Military History, 1997); Stephen I. Vladeck, "Emergency Power and the Militia Acts," *The Yale Law Journal* 114, no. 1 (October 2004), 149–194; and Paul J. Scheips, *The Role of Federal Military Forces in Domestic Disorders, 1945–1992* (Washington, DC: U.S. Army Center of Military History, 2005).

[3] Alexander Hamilton, Federalist No. 29 (January 9, 1788).

[4] For opposing views on its applicability to Presidential action in domestic disorders, see Monaghan, "The Protective Power of the Presidency"; Oren Gross, "Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?" *Yale Law Journal* 112, no. 5 (February 2003), 1011–1134; and Andrew Kent, Ethan J. Leib, and Jed Handelsman Shugerman "Faithful Execution and Article II," *Harvard Law Review* 132, no. 8 (June 2019), 2111–2192.

[5] For the discussion in the House of Representatives, see *Annals of Congress*, House of Representatives, 2nd Cong., 1st sess., 574–580. On May 2, 1792, Congress approved "An Act

to provide for calling forth the Militia to execute the laws of the Union, suppress insurrections and repel invasions," *Acts of the Second Congress of the United States* (Philadelphia: Francis Childs and John Swaine, 1793), 264–265. This act is known as the Calling Forth Act.

[6] "An Act to provide for calling forth the Militia to execute the laws of the Union, suppress insurrections and repel invasions," 264.

[7] David E. Engdahl, "Soldiers, Riots, and Revolution: The Law and History of Military Troops in Civil Disorders," *Iowa Law Review* 57, no. 1 (October 1971), 1–73, quoted on 44.

[8] "An Act to provide for calling forth the Militia to execute the laws of the Union, suppress insurrections and repel invasions," 264.

[9] Ibid.

[10] Ibid., 265.

[11] See Leland D. Baldwin, *Whiskey Rebels: The Story of a Frontier Uprising* (Pittsburgh: University of Pittsburgh Press, 1939), for the most authoritative account.

[12] Vladeck makes the important point that each branch abided by its roles and responsibilities in the 1792 militia in "Emergency Power and the Militia Acts," 161.

[13] On February 28, 1795, Congress approved "An Act to provide for calling forth the Militia to execute the laws of the Union, suppress insurrections and repel invasions; and to repeal the Act now in force for those provisions," *Acts of the Third Congress of the United States* Philadelphia: Francis Childs and John Swaine, 1794), 424–425. This act is known as the Calling Forth Act.

[14] See Vladeck, "Emergency Power and the Militia Acts," 163, for a discussion on the removal of these checks on authority.

[15] Wilson, *Federal Aid in Domestic Disturbances, 1787–1903*, 45–49; Coakley, *The Role of Federal Military Forces in Domestic Disorders, 1789–1878*, 77–83; George M. Dennison, "Martial Law: The Development of a Theory of Emergency Powers, 1776–1861," *American Journal of Legal History* 18, no. 1 (January 1974), 56–59.

[16] Coakley, *The Role of Federal Military Forces in Domestic Disorders, 1789–1878*, 83 n46. Also see Dumas Malone, *Jefferson the President, Second Term, 1805–1809* (Boston: Little, Brown, Co., 1974), 252–253. The full text is available in *Acts of the Ninth Congress of the United States* (Washington, DC: Authority, 1807), 443.

[17] U.S. Reports: *Martin v. Mott.*, 25 U.S. (12 Wheat.) 19 (1827), 31.

[18] Alan Hirsch, "The Militia Clauses of the Constitution and the National Guard," *University of Cincinnati Law Review*, No. 59 (1988), 950–956.

[19] U.S. Reports: *Luther v. Borden et al.*, 48 U.S. (7 How.) 1 (1849), 44.

[20] Ibid., 45.

[21] Dennison, "Martial Law," 76; Wilson, *Federal Aid in Domestic Disturbances, 1787–1903*, 291–292; and Coakley, *The Role of Federal Military Forces in Domestic Disorders, 1789–1878*, 34–36.

[22] Edward Bates, "Suspension of the Privilege of the Writ of Habeas Corpus," 10 Ops. of Att. Gens., 74–92 (1861); Bates letter, July 5, 1861. Emphasis added.

[23] James G. Randall, *Constitutional Problems Under Lincoln* (New York: D. Appleton & Co., 1926), 48–73, would describe this as part of Lincoln's dual theory of the war, both an insurrection and an international conflict.

[24] Ibid., 243.

[25] U.S. Reports: *Prize Cases*, 67 U.S. (2 Black) 635 (1863), 670.

[26] On April 20, 1871, Congress approved "An Act to enforce the Provisions of the Fourteenth Amendment to the Constitution of the United States, and for other Purposes," *Acts of the Forty-Second Congress of the United States* (Washington, DC: Government Printing Office, 1872), 13–15. This is known as the Third Enforcement Act, the Ku Klux Klan Act, and the Civil Rights Act of 1871.

[27] C.C. Andrews, ed., *The Attorneys General of the United States, Advising the President and Heads of Departments, in Relation to Their Official Duties*, vol. 6 (Washington, DC: W.H. & O.H. Morrison, 1871), 473. Also see Coakley, *The Role of Federal Military Forces in Domestic Disorders, 1789–1878*, 132–133.

[28] See the culminating discussion in the Senate on June 7, 1878, in 7 *Congressional Record*, 4239-4248. Also, Laurie and Cole, *The Role of Federal Military Forces in Domestic Disorders, 1877–1945*, 18–21. The entire body of Federal law was codified in the 1874 Revised Statutes. Four of these statutes (5297, 5298, 5299, and 5300) dealt with Federal aid to civil authorities and insurrections against either state or Federal authority.

[29] *Acts of the Forty-Fifth Congress of the United States* (Washington, DC: Government Printing Office, 1878), 144.

[30] Laurie and Cole, *The Role of Federal Military Forces in Domestic Disorders, 1877–1945*, xx.

[31] U.S. Reports: *In re Debs*, Petitioner, 158 U.S. 564 (1895), 582.

[32] Laurie and Cole, *The Role of Federal Military Forces in Domestic Disorders, 1877–1945*, 277–301; William Cohen, "Riots, Racism, and Hysteria: The Response of Federal Investigative Officials to the Race Riots of 1919," *Massachusetts Review* (Summer 1972), 373–400.

[33] Laurie and Cole, *The Role of Federal Military Forces in Domestic Disorders, 1877–1945*, 255–275.

[34] *Acts of the Fifty-Seventh Congress of the United States* (Washington, DC: Government Printing Office, 1902), 775–780. In 1916, Congress further distinguished the militia as organized (National Guard and Naval Militia) and unorganized. This latter definition remains in 10 *U.S. Code* 246 today.

[35] U.S. Reports*: Youngstown Co. v. Sawyer*, 343 U.S. 579 (1952).

[36] Ibid. Black suggested that the government had two relevant statutory mechanisms through the Selective Service Act (1948) and Defense Production Act (1950) to take action, but the government did not pursue them for expediency reasons.

[37] U.S. Reports: *Youngstown Co. v. Sawyer*, 343 U.S. 579 (1952), 587.

[38] Ibid., 632.

[39] Ibid., 644–645.

[40] Ibid., 637.

[41] Ibid., 644–645.

[42] Laurie and Cole, *The Role of Federal Military Forces in Domestic Disorders, 1877–1945*, 421–425.

United Nations forces withdraw from North Korean capital, Pyongyang, recrossing 38th parallel, ca. 1950 (U.S. Information Agency/U.S. National Archives and Records Administration)

More Afraid of Your Friends Than the Enemy

Coalition Dynamics in the Korean War, 1950–1951

By Fideleon O. Damian

Collaboration with other countries is an integral part of the U.S. National Security Strategy. Its most recent version notes that "allies and partners are a great strength of the United States" that "add directly to U.S. political, economic, military, intelligence, and other capabilities."[1] Since the end of the Cold War, countries have preferred to collaborate through coalitions rather than formal alliances because the latter are more liable to impose political constraints. Coalitions, according to Patricia Weitsman, are "ad

Fideleon O. Damian is a Military Analyst working in the Washington, DC, metropolitan area.

Men and equipment parachute to ground in operation conducted by United Nations airborne units, ca. 1951 (DOD/U.S. Information Agency/U.S. National Archives and Records Administration)

hoc multinational undertakings that are forged to undertake a specific mission and dissolve once that mission is complete."[2] Weitsman claims that coalitions tend to be more cohesive than formal military alliances because of their ad hoc nature, the ability of the coalition leader to tailor membership to suit the mission, and, most relevant to this article, the absence of formal institutions and consultative processes found in formal alliances.[3] This viewpoint suggests that coalition members do not need to prepare for cases where strategic divergences occur or to develop mechanisms to manage a member's internal dynamics.

This article argues that military and civilian leaders should recognize the potential for strategic divergences between

coalition partners and be ready to manage them; it uses as a case study the relationship between the United States and its primary Western coalition partner, the United Kingdom (UK), during the Korean War. The United States and the UK joined the United Nations (UN) coalition during the summer of 1950 with their interests initially aligned around a common goal: the defense of South Korea from communist aggression. By the end of 1950, however, the UK concluded that U.S. actions that could intentionally or unintentionally escalate or broaden the conflict posed a more imminent threat than communist military operations.[4] In response, the UK acted to prevent any U.S. operational or diplomatic initiatives that the British judged as harmful to their national aims. Throughout the

winter of 1950 to 1951 and the following spring, to maintain coalition cohesion, the United States had to reassure its partner that it would prosecute the conflict within military and diplomatic parameters acceptable to the British.

Given the importance of international partnerships to U.S. security strategy, policymakers and scholars should look to the past for lessons on how to form and run coalitions. Studies of coalition dynamics often gravitate toward models of success rather than failure for their insights. Of the prior century, the two most prominent successes often cited as models to emulate are the Allied coalition to defeat Germany and Japan in World War II and the U.S.-led coalition to expel Iraq from Kuwait in the Gulf War.[5] In both cases, the outcomes were unqualified successes,

and the coalition members managed to maintain general alignment at least until the coalition achieved its military goals. However, cases that produced more ambiguous results and internal tensions over the conduct and direction of the conflict, such as the Korean War, merit equal attention for the insights they can provide in today's more complex strategic environment.

Between 1951 and 1953, the United States and the UK fought as part of a UN coalition to prevent a communist takeover of the entire Korean Peninsula. The war began with Soviet-sponsored North Korea invading south of the 38th parallel in June 1950 and nearly succeeding in conquering the whole of South Korea save a small enclave near Pusan. A UN counterattack in September 1950 shattered the North Korean military's fighting capabilities and liberated all the territory lost the previous summer. The UN decision to advance north of the 38th parallel, however, prompted China to intervene on North Korea's behalf and raised fears that UN forces would evacuate the peninsula. By spring 1951, UN forces had recovered sufficiently, and the conflict settled into a protracted war of attrition that ended after 2 years of negotiations produced, in July 1953, an armistice that restored the status quo antebellum.

Korea itself was a largely peripheral strategic issue to both the United States and the UK in summer 1950, and both nations joined the UN coalition less concerned with the outcome on the peninsula itself than with its implications for Anglo-American global cooperation and the opportunity to advance their national ambitions. For the UK, Asia ranked lower than continental Europe in national priorities; within Asia, the survival of South Korea ranked below continued control over its two imperial colonies, Hong Kong and Malaya. Similarly, for the United States, Asia ranked lower than Europe, and South Korea ranked lower than the security of Japan, Taiwan, and the Philippines in the region. Kim Il-sung's invasion and the possible reunification of the peninsula under the communist banner, however, transformed Korea from a

peripheral issue into a Cold War litmus test of Western resolve and solidarity.[6]

The United States and the UK viewed Korea as a bellwether for Anglo-American cohesion on more critical issues at the beginning of the war. Both nations assessed that Korea would test the credibility of its commitment to anticommunism. Each government judged that the failure to counter communist aggression in Asia would encourage even bolder activity by the Soviet Union elsewhere. The United States and the UK also recognized that although Korea was a peripheral global interest, the absence of a coordinated response would serve as an unfortunate omen for future cooperation on higher stakes issues. The two nations considered the Korean crisis a test of the principle of collective security and the legitimacy of the newly established UN as the guarantor of the post–World War II order. Lastly, neither nation wanted a war in Korea to expand into a broader conflict with China or the Soviet Union.[7]

Anglo-American cooperation in Korea was based as much on self-interest as it was on shared interests. The Americans wanted additional partners in the coalition in order to reduce the demands on their military resources. British participation also strengthened the U.S. message that the intervention was an internationally sanctioned response to a threat to global stability, providing the Harry S. Truman administration with domestic and international political legitimacy. The British expected that their support in Korea would prompt the Americans to reciprocate with a stronger commitment to the defense of Western Europe. The British also calculated that despite unquestionable U.S. military and economic superiority, participation would build political capital and goodwill that they could use to steer the Americans to act responsibly and in ways that did not jeopardize British interests.[8]

On paper, though, the British appeared unlikely to challenge U.S. coalition leadership against the balance of overwhelming U.S. political and military power and shared objectives. For example, the United States supplied an entire field army of several hundred thousand

men—compared with the two UK brigades of less than 10,000 men total who depended on U.S. logistics and supply assistance.[9] Outside of Korea, the UK also needed U.S. assistance to advance its nuclear weapons research, to rebuild its shattered economy, and to defend the European continent against potential Soviet aggression.[10]

The British did have reservations about aligning themselves too closely with the Americans, but those concerns were secondary in the British strategic calculus until the Chinese intervention. As much as the UK valued the Anglo-American relationship and its access to U.S. military and economic support, the British were equally uncertain whether U.S. leadership would prevent a third world war or instigate it. Differences over the legitimacy of the Chinese communist government was another area of departure that would have consequences for Anglo-American relations as the war progressed. The United States still considered Chiang Kai-shek's nationalists in Taiwan the legitimate government of China; however, the UK, in order to maintain its economic interests in China and its control over Hong Kong, recognized Mao Zedong's government in January 1950.[11] Once the Chinese entered the conflict, the British feared that Mao would move against their Asian interests, and such concerns likely contributed to the resistance to provoking him directly.

Chinese Intervention Catalyzes a Strategic Rift

The Chinese counterattack in the winter of 1950–1951 shattered UN hopes of an imminent victory and triggered the British loss of confidence in U.S. leadership, which prompted the UK to act to protect its strategic interests. After the entire Korean Peninsula was nearly lost in summer 1950, a successful UN counterattack—combining an amphibious assault at Inchon with an Eighth Army breakout from the Pusan perimeter that September—broke the North Korean military's back. Buoyed by this drastic reversal of fortune and seeing an opportunity to roll back communism, President Truman secured UN approval to expand the conflict beyond the

defense of South Korea. The new aim was to reunite the peninsula under the aegis of a U.S.-sponsored government instead of merely containing the spread of communism.

Beginning in October 1950, Chinese "volunteers" entered Korea to prevent the consolidation of the peninsula under a U.S.-backed government.[12] Although the first skirmishes occurred in late October, the most serious blows fell on November 27, when a Chinese counterattack caught complacent UN forces off guard and sparked a panicked retreat south. The next day, General Douglas MacArthur announced that he faced an "entirely new war" with the entry of more than 200,000 Chinese troops.[13] By mid-January 1951, UN forces had retreated across the 38th parallel and abandoned Seoul, undoing much of the previous autumn's gains.

The UN military position stabilized after a change of command in the Eighth Army and the loss of momentum in the Chinese offensive due to overtaxed logistics.[14] After assuming command of the Eighth Army following Lieutenant General Walton Walker's death in an accident, Lieutenant General Matthew Ridgway replaced ineffective unit commanders and restored troop morale, enabling the UN coalition to steady its battlefield positions. By mid-January, it was clear that the Chinese were having difficulty sustaining their advance after weeks of combat and needed time to reorganize their personnel and logistics. By late January, UN forces had sufficiently recovered under Ridgway, launching offensives that would eventually retake Seoul and return UN positions to the 38th parallel.

The UK Fears the United States More than China

Despite the improved military situation by February 1951, the British ceased showing Washington deference and began taking action to protect their national interests; they had lost confidence that the Truman administration would not expand the conflict.[15] Five factors contributed to this strategic divergence:

- the lack of preparation by the UN coalition for drastic changes to the strategic environment
- UN Supreme Commander MacArthur's influence in decisionmaking
- the minimal weight given to British input into coalition decisionmaking
- the U.S. domestic political environment
- British perceptions that Washington was vulnerable to strategic mistakes.

The British feared that these factors would lead to a miscalculation that would draw the coalition into a direct war against the Chinese and possibly a more openly and directly involved Soviet Union.

The UN coalition's collective inability to anticipate a Chinese intervention or prepare responses probably played no small part in British fears that additional miscalculations were in play. Although Truman and his senior advisors had raised the possibility that the Chinese could enter the conflict if UN forces pressed beyond the 38th parallel, MacArthur assured them that a large-scale intervention was unlikely.[16] Neither back-channel communications from Mao's government nor U.S. intelligence assessments warning of a possible Chinese intervention was deemed of sufficient specificity to challenge the field consensus that the People's Republic of China would not respond with a significant military action.[17] London had passed on to Washington warnings, received through New Delhi as early as September 27, that the Chinese would enter the conflict if the United States crossed the 38th parallel.[18] It appears, however, that up until the Chinese intervened in force in November, London and Washington were uncertain whether it would occur.[19] While Washington and London agreed an intervention would risk escalating the war, the focus of discussion was how to dissuade the Chinese from entering it.[20] The two governments also do not appear to have substantively discussed how the coalition would deal with the fallout of Chinese actions or the implications for the coalition itself.

Another factor behind London's loss of confidence was its discomfort about MacArthur's influence over decisions and its uncertainty of whether Truman or MacArthur was dictating Washington's Korea policy and strategy. The British probably feared that the Truman administration's inability to control the general left the door open for MacArthur or his allies to force an escalation. Following a meeting with Secretary of State Dean Acheson in mid-November, British ambassador Oliver Franks assessed that internally the Secretary of State lacked the power or will to convince the Joint Chiefs of Staff (JCS) to pay less deference to MacArthur's decisionmaking.[21] In a November 22 telegraph, British foreign secretary Ernest Bevin told Franks that the British House of Commons was concerned that MacArthur's actions could produce a general war with China.[22] Further contributing to London's lack of confidence, Acheson told Bevin on November 24 that a British proposal to the UN establishing a demilitarized zone in North Korea would hurt the morale of UN forces and that it was important all UN members show every possible support to the troops.[23]

The British also assessed that the Chinese intervention resulted from Washington not paying sufficient attention to British perspectives and concerns in their decisions, despite British military contributions to the coalition. Air Chief Marshal Sir William Elliot, the chief staff officer to the Ministry of Defence, informed Prime Minister Clement Atlee after the November 20 meeting that the British chiefs of staff had concluded it was necessary to start presenting their views to the Americans in the "most forcible and unequivocal terms."[24] In his November 22 telegraph to Franks, Bevin informed him that as foreign secretary, he was placed in an awkward situation because British troops fought under UN authority, but London had little say in how the UN commander would use those troops. Bevin assessed that the UK needed to press the United States to consult more with those UN member states supplying forces for the war.[25]

British assessment of U.S. domestic politics further reinforced doubts the

General of the Army Douglas MacArthur inspects troops of 24th Infantry on his arrival at Kimpo Airfield for tour of battlefront, February 21, 1951 (U.S. Information Agency/U.S. National Archives and Records Administration)

Truman administration could keep the war limited. During a November 20 meeting of the British chiefs of staff committee, William Slim, chief of the Imperial General Staff, expressed his concerns that internal U.S. politics were undercutting the Truman administration's ability to contain the scope of the conflict and exercise greater control over MacArthur's operations.[26] By November 25, the British chiefs of staff told Arthur Tedder, the head of the British Joint Services Mission in Washington, that the U.S. domestic climate made it difficult for British diplomats to moderate American behaviors, despite a shared interest in preventing an expansion.[27]

Washington's public messaging probably further raised London's concerns that its coalition leader could make a strategic miscalculation under pressure. During a press conference on November 30, Truman made statements that especially troubled the British and other allies. First, he stated, "We will take whatever steps are necessary to meet the military situation, just as we always have."[28] A follow-on question asked whether this included the use of the atomic bomb, to which Truman replied, "There has always been active consideration of its use." Truman went even further when he stated that the decision to employ atomic weapons rested with the field commander. Although this was certainly not

his administration's policy and Truman subsequently clarified his statements, many in the international community interpreted them as a threat to escalate and use the bomb.[29] The haste with which Truman spoke and then backtracked his statements probably did little to reassure British decisionmakers that they could unconditionally rely on Washington to have the internal clarity and prudence to make sound strategic decisions.

The Consequences of Strategic Divergence: Preventing a Wider War

It was clear that by late November, the UK had lost confidence that the United States could keep the war

Clockwise from lower left, President Harry S. Truman, Secretary of State Dean Acheson, Secretary of Defense George C. Marshall, and Prime Minister Clement Attlee, at the White House, Washington, DC, December 6, 1950, autographed by President Truman (Courtesy Harry S. Truman Library & Museum/National Park Service/Abbie Rowe)

limited and would not escalate by design or accident. The UK had also lost confidence that its strategic interests were safe. The fear and uncertainty created by the American response to the Chinese intervention was the final straw that prompted the UK and other allies to move to protect their national interests against any U.S. actions that had the potential to escalate the war.[30] Truman's press conference on November 30, 1950, especially catalyzed the British to take more active and direct measures. From December 1950 to May 1951, as long as the British feared that their coalition leader could control the situation, the UK exercised what influence it could to prevent the United States from expanding the war.

More important, British fears had risen to the point that the UK was willing to risk damage to Anglo-American relations by publicly breaking with the United States in the UN.

Between December 1950 and May 1951, the UK took action to counter or delay potential American actions, two in the military sphere and one in the political, that could harm its strategic interests. First, the British worried that the United States would employ atomic weapons. Second, the Atlee government feared that the Truman administration would succumb to MacArthur's demands to bomb Manchuria. Finally, London was concerned that the United States could push for punitive UN resolutions against China. The British concluded that by

engaging with the United States to force it to address their concerns, they could at least stall—and, if necessary, block—the United States from taking actions that London viewed as damaging. From the British perspective, these actions would compel the Americans to consider an alternative view of the risks they were taking and the possible unintended consequences.

The British leveraged the Truman-Atlee meetings of December 3–8, 1950, to voice concerns over the use of atomic weapons and to enhance British prestige in the relationship.[31] Although the United States had no immediate intentions to employ the atomic bomb at the time of Atlee's visit, Truman's November 30 statements had made it necessary for

the UK to seek assurances on U.S. intentions regarding atomic weapons. The minimum American concession Atlee hoped for, initially, was Truman's commitment that any use of atomic weapons would involve consultations with the British government. After being informed of the domestic unfeasibility of such a proposal by Acheson, Atlee was satisfied with a public commitment by Truman that expressed his hope that circumstances would "never call for the use" of atomic weapons. Truman also promised he would "keep the Prime Minister at all times informed of developments which might bring about a change in the situation."[32]

While the Truman-Atlee conference seemed to assuage immediate concerns over atomic weapons, the British still feared they would find themselves in a broader war if the United States expanded the air conflict into Manchuria. Of particular concern to the British were U.S. proposals to give the UN commander permission to conduct "hot pursuit" of communist aircraft attacking UN troops over the Yalu River and into Manchuria. MacArthur was still the UN commander when the British rejected an additional U.S. proposal on April 6, 1951, to allow retaliatory bombings of airbases in Manchuria that were the origin of Chinese air attacks. London requested that Washington instead first consult its allies and issue a warning to the Chinese to cease air attacks before crossing into Manchuria.[33] The British assessed that giving MacArthur the authority to conduct either kind of air action risked widening the war.[34] Even after MacArthur's removal later that month, the British refused to accept American proposals unconditionally and insisted on having some input out of fear that Truman could authorize a drastic action in response to domestic pressure. Although the Pentagon would later give MacArthur's replacement, Ridgway, authority to conduct retaliatory air attacks, the instructions the JCS issued acknowledged allied sensitivities. Ridgway had to consult with the JCS before authorizing any strikes; if this was not feasible, he was to inform the JCS as soon as possible and

avoid discussing the matter publicly until Washington had notified its allies. By insisting any decisions regarding airstrikes in Manchuria involve other coalition partners, the British had gained some additional ability to influence and prevent a hasty action that could drag them into a wider war.

Equally concerning to the British was an American demand for a UN resolution to condemn China as an aggressor and impose punitive sanctions. Passage of such a resolution risked hardening Chinese resolve and undercutting efforts by the British and others to negotiate a ceasefire.[35] The British became aware of the U.S. intent to call for a UN resolution condemning China at the end of December 1950 after the State Department began soliciting support from member states for the measure. Working together with Canada, the UK started building support within the UN and with its Commonwealth to delay passage of such a resolution.[36] First, the British delayed the resolution's proposal until January 20 by convincing the United States to allow China to accept a UN statement of principles for a ceasefire first.[37] Next, the British stalled passage of the U.S.-backed UN resolution by objecting to language that implied authorization for economic sanctions against China, which the British feared would only provoke the Chinese. The British were sufficiently concerned about the resolution that they were willing to publicly break with the United States and vote against its passage unless the United States addressed their concerns.[38] Recognizing that a public "no" vote by the British could prompt a domestic political backlash and undermine U.S. congressional support for the more strategically important rearmament of Europe, the Truman administration amended the resolution with additional language to assure the British that any proposed sanctions against China would be brought to the UN first.[39]

The most important outcome of British actions was that London was able to protect national interests by diminishing the possibility that the United States could unilaterally escalate the conflict.

While some scholars have argued that British efforts had minimal influence on U.S. decisionmaking or consequences regarding China, these claims do not give the British sufficient credit in reducing the prospects of a U.S. miscalculation. For example, Callum MacDonald has argued that the United States had no intention of expanding the war and that the UK would have had little capability to prevent the United States from doing so even if it had.[40] Although Peter Lowe has argued that British fears were valid and the winter of 1950–1951 was the closest the United States ever came to using atomic weapons in Korea, he also claims that British dependency on the Americans hindered UK capacity for independent action.[41] William Stueck, however, contends British and UN members did reduce the chances of expanding the war because they sufficiently delayed the United States from a hasty overreaction and created the space and time for the military situation to stabilize. These improved battlefield conditions reduced the pressure on Truman to authorize a drastic action to salvage the U.S. position.[42] Though British actions alone were not decisive in ensuring the Korean War did not escalate further, they did make it more difficult for the more powerful ally to drag the UK into a broader conflict unintentionally and without at least considering the ramifications of such actions.

Another important consequence of the UK actions was that U.S. political and military strategic decisionmaking in the war became less unilateral and paid more attention to internal coalition strategic concerns to maintain cohesion. According to Stueck, after the winter of 1950–1951, the Truman administration probably lost the latitude to employ measures that could have forced the communists to agree to an armistice earlier, because of the Atlee government's resistance.[43] Although using atomic weapons, bombing Manchuria, or other militarily expedient actions could have changed the military balance, the British by their actions made it clear the United States would have to risk paying a high political cost if the Truman administration acted unilaterally and without deliberation.

If the United States was willing to go beyond what its allies deemed prudent, it would have to consider whether the action merited a public break with its partners that would undermine U.S. claims that it was acting in Korea to defend the international order.

Recommendations

Although they occurred nearly seven decades ago, the tensions in the U.S.-UK coalition during the winter of 1950–1951 offer several salient lessons on what future warfighters and policymakers should consider when attempting to mitigate strategic divergences among coalition members. It is impossible to prevent all friction; however, devoting more time and attention to managing coalition relationships in strategy formation and execution could reduce the risk of members working at cross-purposes during periods of acute crisis. These lessons are equally valid for ad hoc groupings assembled for a specific objective and permanent formalized alliances.

Embrace the Complexity of Coalitions to Manage Them Better. Quantifiable aspects such as money, troops, and weapons platforms provide readily identifiable metrics to understand relative importance within a coalition and the advantages gained from being in one; however, policymakers and planners must appreciate the complex nature of coalitions to manage them effectively. As the Korean War example illustrates, the influence and importance of a coalition member are not gauged in quantifiable, proportionate, or direct terms. Current strategic leaders should recognize that quantifiable factors mask other dynamics that carry with them outsize benefits and costs. When working with a coalition partner, choices should be made based on the strategic value of the relationship, of which military forces are only one dimension. Both parties in the Anglo-American relationship recognized the value of the British participation as being more than just men and materiel, and this meant the consequences of failed cooperation in Korea would extend into immediate and longer term strategic matters. Without

this recognition, the American imperative to address British concerns might not have emerged.

Interagency Cooperation Will Be Crucial to Managing Complexity. A coalition is as much a diplomatic relationship as it is a military one—and needs strategic leaders who are comfortable operating in both realms. Warfighters will need to pay as much attention to diplomatic initiatives as they do to military operations in the field (and vice versa for diplomats). Furthermore, proper management of this complexity will likely require coordination across the spectrum of government to ensure all activities complement each other. Effective strategic leadership will require leaders who are educated in thinking broadly about issues and capable of working across government agencies.

Address Partner Concerns over Politically Driven Changes to Coalition Dynamics. Military and civilian strategic decisionmakers alike should recognize that coalition partners pay attention to domestic politics and need to be reassured once differences emerge. Planners and policymakers must be ready to take preemptive actions to assuage and reassure coalition partners when domestic trends seen as harmful for the coalition's cohesion and partners' interests emerge. The British astutely observed that a U.S. President's ability to control policy had limits and that, with sufficient public outcry, political opponents in Congress or military leaders such as MacArthur could compel Truman to take measures he did not want to employ or in haste. If political forces of a coalition partner are driving events in a direction that could affect the broader coalition, then that coalition member should do what it can to include partners in shaping a collective response.

Coalitions Should Have Contingency Plans and Processes to Deal with Major Recognized Potential Strategic Shifts. Much of the tension between the United States and the UK emerged because of the sudden strategic shock of China's entry into the war. Although it is impossible to predict everything that could happen in war,

both the United States and the UK considered the possibility of Chinese intervention and recognized it would have significant strategic implications. Despite such mutual concern, apparently no in-depth discussion took place on what Chinese intervention would mean for the broader coalition or how it would respond. When a coalition member raises a possible strategic development of concern, the prospects and the implications should be deliberated with some rigor. In their strategic planning, coalitions should at least have mechanisms in place to consider the conditions under which these developments could occur, how such an event would influence their participation, and what modifications to overall strategy and operations members would accept.

Coalitions Members Should Work to Reinforce Harmony, Even Among Historical Partners—Absent Effort, Relationships Risk Decaying. Dominant members of a coalition should not take for granted that past goodwill will persist indefinitely. When deciding how much to consult with coalition partners, prudence dictates erring on the side of more consultation, reassurance, and engagement. When circumstances require rapid responses that prevent extensive deliberations, the preexisting trust and goodwill built by earlier engagements become all the more vital in providing reassurance that members will act responsibly and to the coalition's benefit. Despite a recent history of close collaboration, close cultural ties, and close personal ties among senior leaders, disagreements and tensions still developed between the Americans and British. Both the United States and the UK had domestic political considerations and their national interests to factor into their respective strategic calculus, and when one party perceived the two were falling out of alignment, it acted to protect those interests. While the United States did wield tremendous political and economic levers to influence behavior, it is essential not to underestimate the effects of constant engagement across all levels of government in easing British fears.

Conclusion

Although the United States is unlikely to experience an imminent, direct military challenge to its hyperpower status, cooperation with other friendly nations in U.S.-led coalitions will be vital to our ability to respond when that moment arrives. What this study has shown is that even disproportionately powerful nations can face challenges to their leadership and limitations to their ability to act unilaterally when their actions pose a risk to their partners. Cases such as Korea could be useful for anticipating the security challenges that lie ahead because the volatility, uncertainty, complexity, and ambiguity that shaped Anglo-American relations seven decades ago will continue to define the strategic environment. Furthermore, future conflicts will almost certainly involve the United States working with multiple coalition partners, who in some cases will have longstanding histories of mutual antagonism and mistrust of one other.

Leading coalitions will place heavy burdens on the United States, but the current reality is that it cannot meet the looming challenges of transnational threats, regional upstart regimes, and revisionist peer/near-peer challengers alone. Prudence dictates that rather than waiting until the actual crisis occurs, future leaders should begin preparing and asking difficult questions now about how we can better manage our coalitions against these threats. History shows us that a better understanding of the nature of the challenges that lie ahead is essential to being prepared to deal with them when the time comes. Moreover, as this article has shown, looking at cases of friction and difficulty between partners can provide insights that just looking at unambiguous strategic successes cannot. Further study into other such cases could help better inform our ability to anticipate and manage these challenges. **JFQ**

Notes

[1] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 37.

[2] Patricia A. Weitsman, "Wartime Alliances Versus Coalition Warfare: How Institutional Structure Matters in the Multilateral Prosecution of Wars," *Strategic Studies Quarterly* 4, no. 2 (Summer 2010).

[3] Ibid.

[4] Thomas Hennessey, *Britain's Korean War: Cold War Diplomacy, Strategy, and Security, 1950–53* (Manchester: Manchester University Press, 2015), 3–4, 108–166; William Stueck, *The Korean War: An International History* (Princeton: Princeton University Press, 1995), 127–157, 330–347.

[5] For examples, see Mark A. Stoler, "The Grand Alliance in World War II," and Richard Swain, "The Gulf War, 1990–1991: A Coalition of Convenience in a Changing World," in *Grand Strategy and Military Alliances*, ed. Peter R. Mansoor and Williamson Murray (Cambridge: Cambridge University Press, 2016), 136–165, 343, 375.

[6] Dean Acheson, *The Korean War* (New York: Norton, 1971), 16–34; Anthony Farrar-Hockley, *The British Part in the Korean War*, vol. 1: *A Distant Obligation* (London: Her Majesty's Stationery Office, 1991), 1–33, 83–105; Hennessey, *Britain's Korean War*, 17–44, 331–348; Harry S. Truman, *Memoirs*, vol. 2 (Garden City, NY: Doubleday and Company, 1956).

[7] Acheson, *The Korean War*, 16–34; Farrar-Hockley, *The British Part in the Korean War*, vol. 1, 1–33, 83–105; Hennessey, *Britain's Korean War*, 17–44, 331–348.

[8] Acheson, *The Korean War*, 16–34; Farrar-Hockley, *The British Part in the Korean War*, vol. 2, 1–44, 83–105; Truman, *Memoirs*, vol. 1, 331–348.

[9] Jeffrey Grey, *The Commonwealth Armies and the Korean War: An Alliance Study* (Manchester: Manchester University Press, 1990), 167–181.

[10] Farrar-Hockley, *The British Part in the Korean War*, 1–33, 83–105.

[11] Hennessey, *Britain's Korean War*, 12.

[12] Truman, *Memoirs*, vol. 2, 376.

[13] Quoted in Acheson, *The Korean War*, 73; Hennessey, *Britain's Korean War*, 100.

[14] William Stueck, *Rethinking the Korean War: A New Diplomatic and Strategic History* (Princeton: Princeton University Press, 2002), 126–127.

[15] Hennessey, *Britain's Korean War*, 3–4, 108–166; Stueck, *The Korean War*, 127–157.

[16] Allan R. Millett, *The War for Korea, 1950–1951: They Came from the North* (Lawrence: University Press of Kansas, 2010), 297–299.

[17] Ibid.

[18] Stueck, *The Korean War*, 90–91.

[19] Stueck, *Rethinking the Korean War*, 117; Hennessey, *Britain's Korean War*, 69–104.

[20] Hennessey, *Britain's Korean War*, 69–104.

[21] Ibid., 90.

[22] Ibid., 93.

[23] Ibid., 96.

[24] Ibid., 91.

[25] Ibid., 93.

[26] Ibid., 90.

[27] Ibid., 98.

[28] Truman, *Memoirs*, vol. 2, 395.

[29] Ibid.

[30] Stueck, *The Korean War*, 130–132.

[31] Ibid., 138.

[32] Hennessey, *Britain's Korean War*, 127–128; Truman, *Memoirs*, 413.

[33] Stueck, *Rethinking the Korean War*, 129.

[34] Ibid.

[35] Stueck, *The Korean War*, 151–153.

[36] Ibid., 151–152.

[37] Ibid., 152–154.

[38] Hennessey, *Britain's Korean War*, 159–166.

[39] Stueck, *The Korean War*, 155–156.

[40] For an example, see Callum MacDonald, *Britain and the Korean War* (Oxford: Basil Blackwell, 1990).

[41] Peter Lowe, *Containing the Cold War in East Asia: British Policies Towards Japan, China, and Korea, 1948–53* (Manchester: Manchester University Press, 1997).

[42] Stueck, *Rethinking the Korean War*, 129.

[43] Peter Stueck, "The Korean War," in *The Cambridge History of the Cold War*, vol. 3, ed. Melvyn P. Leffler and Odd Arne Westad (Cambridge: Cambridge University Press, 2010), 285–287.
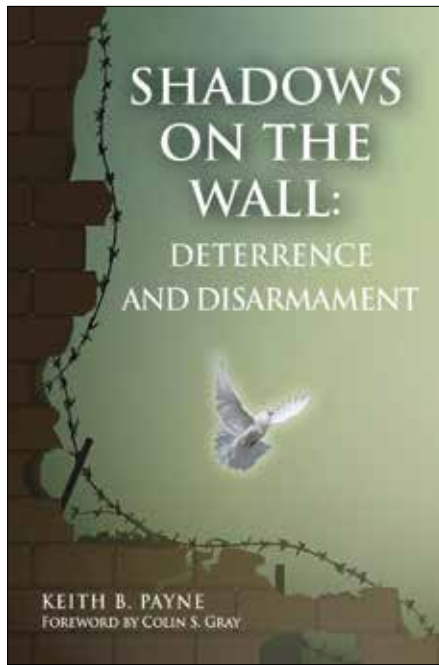
Shadows on the Wall: Deterrence and Disarmament

By Keith B. Payne
National Institute Press, 2020
204 pp. $12.00
ISBN: 978-0985555320

Reviewed by John Mark Mattox

Despite pretentions to the contrary, the academic mind rarely makes room for discussions of first principles—those basic assumptions taught in first-semester undergraduate classes that undergird any given discipline. Instead, the traditional path for the aspiring academic is to obtain a terminal degree, carve out an esoteric research niche, and demonstrate talent by identifying the nuances of the niche. This approach, which the academy has taken ever since there was such a thing as a "terminal degree," is not without merit. The academy does aim to create new knowledge, some of which turns out to be useful. On the other hand, it also breeds cottage industries churning out new, nuanced knowledge for new, nuanced knowledge's (and tenure's) sake in a way that can obscure first principles. As a result, once in a while, someone needs to come in with a chain saw and lop off all the undergrowth that conceals the forest floor. It is that much-needed task that Keith Payne undertakes in *Shadows on the Wall* in the long-established cottage industries surrounding nuclear deterrence and disarmament.

Instead of examining the merits or demerits of myriad policy proposals recycled over decades, Payne returns to first principles—not only to the genesis of the nuclear age but also to the foundations of the international system. He identifies three divergent philosophical paths—each with its own a priori assumptions—from which flow deterrence theories and eventually deterrence policies. While all paths acknowledge the anarchic state of the international system, each contemplates different reactions to that anarchy vis-à-vis nuclear weapons: one idealistic, holding that, despite systemic anarchy, national interests can be subordinated in such a way that all parties would deem nuclear weapons unnecessary; one realistic, holding that, while flawed human nature underlies all expressions of national interest, nuclear deterrence can be achieved relatively easily; and a second brand of realist that regards nuclear deterrence as difficult to achieve as it is necessary. Payne argues that to the extent policy discussions lose sight of these bedrock assumptions, those who disagree on policy directions cannot understand why they and their interlocutors cannot agree or make concessions that would alter landscapes dictated by *Weltanschauung*. In short, the answer to "Why can't you see nuclear policy my way?" must essentially be "Because my foundational views about human nature and the system of nations in which it operates is fundamentally different."

This confusion is compounded by the pseudo-philosophy of the transactional "deal-making" approach to international relations, which ignores the reality that some who pull the levers of power in the world's different polities simply see the world differently. Thus, what may seem obvious from the perspective of the nation that introduced the world to nuclear weaponry may not be so obvious from other vantage points—especially ones that might be interested in reordering the world in terms of a socialism "with Chinese characteristics" or another that wants to introduce weapons based on "new physical principles." The problem is further complicated when blind tribal commitment to pro forma political party positions du jour obscures the reality that questions such because how or whether to deploy nuclear weapons rests on assumptions about human nature that have almost nothing to do with contemporary politics. Hence, Payne suggests that undue focus on these distractions renders almost impossible a proper focus on the basic propositions he reasserts.

While Payne's argument constitutes a good reminder for those who wish to engage in serious policy discourse, his focus is on nuclear weapons. Not unlike Alfred North Whitehead's famous observation that "The safest general characterization of the European philosophical tradition is that it consists of a series of footnotes to Plato," Payne argues compellingly that 75 years of nuclear policy debates are really footnotes to the philosophical views set out by some of the greatest minds of the mid-20th century and the purveyors of nuclear policy change, but nothing is really new.

However, Payne's purpose is not to hinge a critique on this point. Rather, it is to demonstrate that incommensurability within positions on nuclear policy stems not from the personalities or parties in power at any given time but from the most fundamental divergences: "Can one entertain serious idealistic assumptions leading to the disarmament of the international system, or not?" "If one cannot, and assuming that nuclear deterrence is preferable to nuclear war, is deterrence relatively easy or difficult to achieve?" These questions are not trivial, and if joint force planners miss this point, they will be missing *the* point. One might be tempted to respond to Payne by stating, "Yes, but deterrence and disarmament are more complicated than that." However, Payne does not suggest that there are no details to work out or compromises to be made. He simply reminds us not to miss the forest for the trees.

Payne supplements his discussion of first principles with useful tables comparing policies and their outcomes based on the fundamental positions outlined. These comparisons will aid the novice and the expert alike and reveal that deterrence discourse is not necessarily as burdened with nuance as some cottage industrialists assumed. The clarity of this comparative work goes hand in hand with the dutifully researched and well-sourced argumentation. Payne's sweeping command of the full constellation of political science and deterrence theory literature makes him an excellent guide through the undergrowth-cluttered forest, beyond which one must see in order to home in on essential principle.

Shadows on the Wall provides the reader with a rare occurrence—a clear view of the fundamental principles that form the basis of deterrence discourse. Payne does the entire field a service by acknowledging that there is a lot of undergrowth to be removed if one is to understand the essence of what might otherwise seem to be a bewildering array of nuanced policy choices. Joint force policymakers, planners, and national security practitioners would be wise to take up this book and absorb its first principles before any other that claims to expand on the merits or demerits of nuclear deterrence and disarmament policy. **JFQ**

Dr. John Mark Mattox is a Senior Research Fellow in the Center for the Study of Weapons of Mass Destruction, Institute for National Strategic Studies, at the National Defense University.
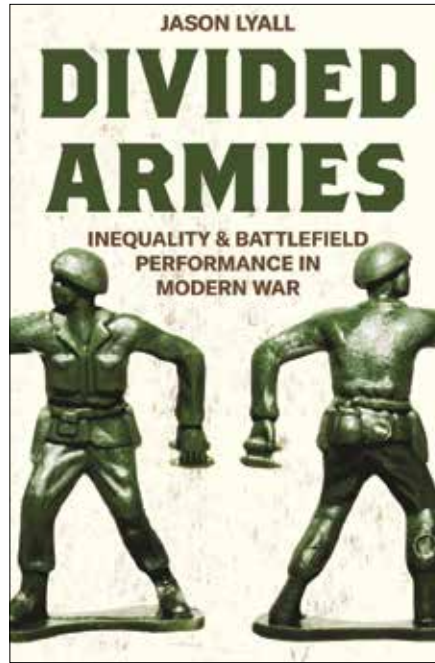
Divided Armies: Inequality and Battlefield Performance in Modern War
By Jason Lyall
Princeton University Press, 2020
528 pp. $35.00
ISBN: 978-0691192444

Reviewed by Larry D. Miller

Why armies win wars or suffer battlefield defeats has long piqued the curiosity and interest of military historians, war planners, and strategists alike. Theorists commonly attribute military effectiveness (or not) to force ratios, firepower, technological superiority, material/resourcing advantages, or exceptional leadership (possibly aided by surprise or dumb luck). Jason Lyall, however, advances a groundbreaking analysis for understanding who wins, who loses, and why. In the process, he suggests equality as a key element in better designing military forces positioned for battlefield success.

His argument is that political communities necessarily and invariably import existing ethnic, racial, religious, and/or societal hierarchies into military organizations—organizations that are political extensions of the state poised to inflict violence. Preexisting inequalities create friction, promote division, diminish organizational cohesion, and undercut battlefield performance to varying degrees. *Military inequality*, a measurable construct introduced by Lyall, is a function of identity as it relates to group membership and relational standing within the political community weighted by inclusion, discrimination, or repression. This concept includes all group members who enjoy full standing, those who are marginalized, those who suffer sanctioned discrimination, and those who experience collective repression. Lyall's extensive, detailed, and well-crafted book effectively demonstrates the validity of his hypothesis and how high levels of military inequality negatively affects battlefield performance. Armies rife with politically sanctioned inequalities, therefore, are flawed by their very design.

The evidence Lyall presents is original and compelling. The opening chapter overviews the genesis of his thinking while detailing essential concepts, terms, and definitions. The balance of the book, eight chapters and two appendices, is organized under three major headings: "Theory and Initial Evidence," "Historic Battlefield Evidence, and "Extensions and Conclusions." The chapters present detailed historiography, quantitative analyses of data drawn from Project Mars, and case studies purposefully selected to challenge and assess the strength of his argument from various angles. Project Mars, the culmination of a 7-year research effort, documents direct force-on-force conflicts between 1800 and 2011. Building the Project Mars database required the support and expertise of 134 coders tracking primary documents and secondary sources across 21 languages. The goal was to construct a global military database documenting armed conflicts in the modern era. Containing 825 observations of belligerence, the database complements, and will possibly supersede, portions of the Correlates of War Project database.

Throughout the book, Lyall employs statistical analyses and historiography—a potent combination of quantitative and

qualitative methods—to assess cross-national military inequality against measures of battlefield performance. Hypothesized expectations include, for example, that as the coefficient of force inequality increases, tactical and operational sophistication will decrease, battlefield fatalities will increase, defections will increase, and coercion and fratricidal violence within the force will rise.

Lyall's detailing of a well-researched conflict in the latter 1800s is particularly illustrative and serves as a preliminary test of his hypothesis. In brief, Muhammad Ahmad (known as the Mahdi) built an inclusive and egalitarian political community from diverse tribes, clans, and ethnic groups in what is primarily present-day Sudan. He assembled an army that defeated Egyptian and Anglo-Egyptian forces during the first Mahdist war (1881–1885). Following the Mahdi's early and unexpected death in 1885, his successor initiated sweeping changes that infused poisonous identity politics into the community. Some tribes and ethnic groups were favored, some were not, and some experienced state-sanctioned repression. In due course, the Anglo-Egyptian forces returned and claimed a resounding victory during the second Mahdist war (1896–1899). Numerous accounts for this reversal of events exist, including arguments about improved weaponry and technological advantages that favored the British. Lyall's careful matching of covariates and contextual variables, however, along with insights from primary and secondary source material, successfully illustrates the "relationship between inequality and battlefield performance."

Divided Armies is an inviting and challenging read, one that necessitates and rewards thoughtful investment. Readers who are unfamiliar with notions of independent variables, covariates, paired comparisons, and regression analysis may find some elements of the discussion obscure and possibly off-putting despite the author's solid and generally successful efforts to deliver a book with minimal technical jargon. Some will also undoubtedly critique the emphasis on land-based operations in

the case data; however, the conclusions are applicable across the joint force. Regardless, the book is well-written and worth the intellectual bandwidth required to parse through the meticulous research.

The joint force will find much to consider in *Divided Armies* as the national security enterprise adjusts to confront 21st-century challenges. Lyall's work suggests inclusivity as a way forward, especially in uncertain times. The future of war is unknown in many respects, but absent full-on technological destruction, one can predict that the tensions between globalization and nationalism will continue, variously propelling and repelling the desirability of diversity within national and international communities. Yet Lyall has convincingly demonstrated that the most successful armies will not only *be* diverse, but they will also *embrace* diversity as strength and use that strength to repel and defeat armies unable to overcome their own inequalities. **JFQ**

Dr. Larry D. Miller is the Director and Professor of Communicative Arts at the U.S. Army War College.
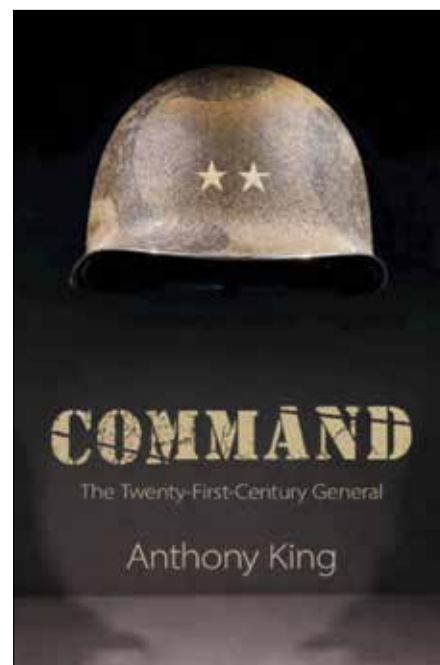
Command: The Twenty-First-Century General

Reviewed by Allan R. Millet

Command is two loosely connected books. One book is about generalship in combat in the 21st century with a focus on hybrid conflicts. The second is about imagining generalship as a collective enterprise and the challenges of employing a division of differently sized units with unique capabilities. A division might be limited to units that shoot and destroy and heavy in units that simply collect and process information with such speed that no single commander could possibly make timely decisions. Drawing on his prior work on unit cohesion and military culture as a British army contractor, Dr. Anthony King offers an updated look at generalship and division command for an increasingly complex battlefield.

Command provides a review of how ground combat divisions developed from World War I to the present, spiced with

examples of "good" division commanders and, less convincingly, why some generals were not so good. King does useful comparative work on the armies of Great Britain, the United States, France, and Germany, stressing system problems not rooted in generals' personal style. He emphasizes operational challenges in actual combat, and he acknowledges that different enemies pose different challenges to a division commander.

The second part of *Command* applies multiple theories of leadership and staff organization to the difficulties of planning and controlling current operations. King does not offer up technological silver bullets as solutions, although he is rooted in a cyber world, so he cannot quite dismiss the notion that we will someday pin stars on an artificial intelligence device and salute it—but the HAL 9000 is not yet here.

Professor King recognizes the power of personality and example by making a distinction between command and leadership. However, this is a distinction without a difference. Lower ranks and citizen soldiers do not know enough to judge professional-operational competence, so sheer courage impresses. Professional troops want a steady flow of ammunition and accurate, prompt artillery fire. They know that even generals in hovering helicopters can be shot down. Today's OH-58 is yesterday's white horse.

Professor King has his own Valhalla of modern major generals, who commanded through delegated authority and undelegated responsibility, shaped by team building. It resembles British battalion "O" groups at a higher level. King's exemplars are General Rupert Smith, General Nick Carter, and General James Mattis. All three, according to King, created centralized decisionmaking systems that still provided subordinate commanders with decisionmaking latitude through vertical and horizontal networks for information-sharing. King champions the "Decision Point" system, which stresses the constant measurement of operations against the newest Rosetta Stone, the commander's intent. The social science jargon aside, all this sounds like "feel good" decision by committee, but King

asserts that focused staff training makes the dispersion and reduction of headquarter staffs more effective and allows better intercommand communications.

Command has many laudable features. One theme deals with a real problem: the evolving exercise of command in complex operational environments that cannot be easily characterized as force-on-force engagements decided by massed firepower and/or technological advantages (for example, information domination). King's guidance to senior commanders is to use decisionmaking systems that produce useful, timely information before crises occur.

However, King fails to address several important 21st-century issues that division commanders do not face often, for example, questions of appropriateness and proportionality in waging war. A division commander would certainly be aware of his own casualties and would try to estimate the effect of enemy casualties. Commander's intent is derivative from strategy, which depends on the goals of the highest political authority. It might be far easier to remove a dictator than to replace him, as General Smith learned in Basra. Smith became an arbiter of an Iraqi civil war, a role no amount of gaming could have solved. I believe General Mattis would agree that his command of the 1st Marine Division during the Iraq War was a drive in the sun compared to General Carter's problems in Afghanistan.

Command would also benefit from a more thorough assessment of the problems of air mission tasking. King admires the Marine Corps system of force integration (protected by Title 10, *U.S. Code*) without explaining that the headquarters of a Marine Air-Ground Task Force provides a single commander for three elements: a ground combat element, an air combat element, and a Service-support element. The operational capabilities of each element depend on the mission. They may range from destroying an enemy armored force to rescuing flood victims in a foreign country. King's national system of command, as conceptualized, might allow rapid deployment but does not provide air-ground integration.

Another complication King might have addressed is the domination of rules of engagement (ROE). I had the good fortune to participate in the exercises Bold Guard and Northern Wedding as a Supreme Allied Commander Atlantic watch officer (twice), to observe the annual Ulchi Focus Lens exercise at Command Post Tango in South Korea, to go on patrol with a British battalion in Ulster, and to discuss at length operations in Bosnia and Kosovo with General Wesley K. Clark while he was still Supreme Allied Commander Europe. In all these situations, however diverse, the ROE shaped operations, not strategy—and for no apparent reason.

Written with senior leaders in mind, *Command* offers useful waypoints for a further discussion of the evolution of generalship, decisionmaking, and division command in increasingly complex environments. It also provides useful nuggets for less senior joint force officers as they consider their own leadership and command style on the 21st-century battlefield. **JFQ**

Colonel Allan R. Millett, USMCR (Ret.), Ph.D., is the Ambrose Professor of History and Director of the Eisenhower Center for American Studies at the University of New Orleans.

CALL FOR ENTRIES

for the

2021 Secretary of Defense and
2021 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 2020–2021 academic year. Students are encouraged to begin early and avoid the spring rush. Final judging and selection of winners take place May 2021, 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/

Coming Soon from NDU Press
Strategic Assessment 2020: Into a New Era of Great Power Competition
Edited by Thomas F. Lynch III

Great Power competition is a framework for understanding interstate relations that dominated geopolitics for centuries prior to World War II. Past GPC eras have featured multiple powerful states jockeying for relative status and position. After lying dormant during a two-decade period of post–Cold War globalization and American international primacy, the dynamics of GPC returned to international relations and security studies in earnest during the late 2010s.

Strategic Assessment 2020 provides an expert and nuanced understanding of the most important emerging dimensions of GPC between the three Great Powers in 2020: the United States, China, and Russia. It establishes that the United States stands atop the triumvirate, with China a rising competitor and Russia vying for top-level prestige while facing clear signs of decline. The Sino-American competitive dyad is likely to be the dominant Great Power rivalry into the future. Chapters focus on the critical activities among these Great Powers and develop major implications for other state actors, nonstate actors, and global institutions.

Authors include scholars from the National Defense University and the Institute for National Strategic Studies who have been directly engaged as thought leaders and policymaking pioneers grappling with the strategic contours of the new era of GPC. Chapters and combinations of chapters will be not only useful for students of national security, international relations, and foreign affairs in an academic setting, but also of great value to policy practitioners.

Have you checked out NDU Press online lately?

With 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**