JFQ Joint Force Quarterly

Issue 112, 1st Quarter 2024

Microgrids for the 21st Century

Focus on U.S. Strategic Command

Accelerating Cyber Leader Development

Joint Force Quarterly

Founded in 1993 ▪ Vol. 112, 1st Quarter 2024
https://ndupress.ndu.edu

Gen Charles Q. Brown, Jr., USAF, Publisher
Lt Gen Michael T. Plehn, USAF, President, NDU

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

Executive Editor
Jeffrey D. Smotherman, Ph.D.

Senior Editor and Director of Art
John J. Church, D.M.A.

Internet Publications Editor
Joanna E. Seich

Copyeditor
Christine Moritz

Book Review Editor
Brett Swaney

Designer
John Mitrione,
U.S. Government Publishing Office

Cover 2 images (top to bottom): Marine participates in Veterans Day Parade in New York City, November 11, 2023 (U.S. Marine Corps/Jacquilyn Davis); Marine Corps drill instructor with Lima Company, 3rd Recruit Training Battalion, leads platoon in warm-up exercises before motivational run at Marine Corps Recruit Depot San Diego, September 21, 2023 (U.S. Marine Corps/Elliott A. Flood-Johnson); Recruits with Hotel Company, 2nd Recruit Training Battalion, complete Day Movement Course during Basic Warrior Training, on Marine Corps Recruit Depot Parris Island, South Carolina, November 14, 2023 (U.S. Marine Corps/Ava Alegria)

In This Issue

Forum

JPME Today

Special Feature

Features

Recall

Book Reviews

JFQ Joint Force Quarterly
Issue 112, 1st Quarter 2024
Microgrids for the 21st Century
Focus on U.S. Strategic Command
Accelerating Cyber Leader Development

About the Cover

Airman 1st Class Chanelle Juhasz, 2nd Security Forces Squadron patrolman, guards B-52 Stratofortress during Global Thunder 19, at Barksdale Air Force Base, Louisiana, November 4, 2018 (U.S. Air Force/Mozer O. Da Cunha)

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

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

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

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

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

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

1st Quarter, January 2024
ISSN 1070-0692

President of Ukraine Volodymyr Zelensky speaks in Verkhovna Rada of Ukraine, in Kyiv, May 3, 2022 (President of Ukraine)

Executive Summary

Many VIPs come to the National Defense University to share their views; recently, the students and faculty had the distinct honor to listen to Ukrainian President Volodymyr Zelensky during his visit to Washington in December. A packed house heard an impassioned speech by a man whom fate, and an aggressor, propelled to national leadership.

The next day I was lucky enough to be teaching some of the students who attended the speech, and I asked them for their impressions of the event. Even the most stoic of my students was impressed by the way in which Zelensky laid out his case for supporting his nation. In an Airman's view, he was looking for a solid wingman in his nation's fight to survive. Everyone in that room knew the United States, our allies, and partners have been on Ukraine's wing for nearly 2 years.

Our lesson that day was on Carl von Clausewitz's concepts, and, as you might expect, many of the students drew connections between the baron's 19th-century writings and today's conflicts. I should not be surprised that some things both in the human condition and in conflict do not change. The cases of the current global conflicts are different in scope from the Napoleonic period, but the impact on those involved and their neighboring states is equally strong.

What seems to be buried from the public discourse about support for Ukraine, which has now been tied to other pressing but manageable issues, such as support for Israel and Taiwan as well as addressing immigration issues related to U.S. border security, is what that European part of our national security we have contributed to gains us as a nation. First, every taxpayer dollar for support to Ukraine finds its way into the U.S. economy because we are paying for our older weapons to be provided to Ukraine for battlefield use. Additionally, those weapons in many cases were already in our stockpiles and paid for years ago and will be replaced by new weapons in the pipeline, in effect a modernization speed-up for our military, which in turn will make it more capable. A similar arrangement one would assume is behind U.S. support to Israel.

In turn, those new systems we would provide to our joint force are built in the United States by American workers, paid for by the taxpayers, and in nearly all districts represented in Congress. By helping Ukraine (and Israel and Taiwan), we get a jobs program for defense and related industry workers. Most importantly, providing aid to Ukraine to fight to defend its country means that at least for the past 2 years and likely longer, U.S. forces are not directly in harm's way. How could any of that "deal" be something an American would be against?

People in Europe at the grassroots level in 1815, 1919, and 1945 knew all too well the result of territorial aggression, as Clausewitz did, having fought in more than 30 battles during that period, a witness to death and destruction on a massive scale. One hopes that the long-term reward for aggressors is defeat. We do live in difficult times that demand a reckoning of what we as a nation really stand for. If the United States wasn't as we believe we are, a shining city on the hill, as President Ronald Reagan stated, why would an embattled Ukrainian president ask for our help? Seems simple from a classic Clausewitz reading as to what should be done.

Our Forum section brings three very interesting articles that range from the theoretical to the application of technology to conflict in the 21st century. Returning *JFQ* author and strategist Lukas Milevski takes us on a deep dive into how gray zone operations might or might not play out. Bringing us out to sea, Diane Zorri and Gary Kessler discuss the impact interference with key electronic precision guidance can have on naval and combined operations. Highlighting the intersection between energy and national defense, Steven Curtis and Peter Rocha offer us some interesting concepts for keeping our forces supported with small power grids.

JPME Today returns with two engaging pieces on hot topics within our colleges, one related to delivery of our education to the next generation of senior leaders and the other on how best to consider those graduates who lead in the cyber domain. From the U.S. Naval War College, Kristin Mulready-Stone helps us to better understand the path we will take to achieving the Chairman's required Outcomes-Based Military Education. As cyber was recently recognized as a warfighting domain, the joint force will need leaders who innately understand how to best leverage our capabilities. Setting out an agenda to do so, Alfredo Rodriguez III offers our war colleges several interesting cyber initiatives to consider beyond today's limited offerings.

JFQ welcomes the opportunity in this edition's Special Feature to present perspectives from another combatant command, the U.S. Strategic Command. In my interview with General Anthony Cotton, he provides us with his perspective on making sure our national strategic nuclear forces are always ready to provide forces as necessary to assure our nation's joint warfighting is successful. Helping us understand the scope of the modern challenges, Thomas Hammerle helps us survey the battlespace in which all forms of deterrence will matter. In discussing how the command views its mission, Kayse Jansen describes the composition of new thinking about the frameworks of strategic deterrence. Reminding ourselves of the dual need for strategic readiness and nonproliferation, Jennifer Bradley helps us see a way both to deter the use of and to control the proliferation of nuclear weapons globally. Concepts are only as good as the capabilities a nation has to support them, and as Patrick McKenna and Dylan Land suggest, setting requirements and having an appropriate accounting for the right number of systems needed is critical to mission success.

In Features, we offer three different "think pieces" that span the spectrum of concerns for the joint force, from intellectual property rights to battlefield medical support to how to tie a political aim to a military objective, as Clausewitz long ago suggested. Describing one of the growing concerns for the joint force, Gerald Krieger walks us through how China views intellectual property rights. Addressing response speed, the critical issue in getting medical support on the battlefield, Jennifer Gurney, Jeremy Pamplin, Mason Remondelli, Stacy Shackelford, Jay Baker, Sean Conley, Benjamin Potter, Travis Polk, Eric Elster, and Kyle Remick lay out the survival chain they believe will best achieve a significant reduction of permanent injury and death from combat. One of the great pleasures I have had in this job is publishing Milan Vego, one of our nation's leading strategic thinkers and professional military education professors, who returns in this issue with his views on how we assure the link between political and military objectives.

We close out this issue with an excellent Recall article and three informative book reviews. In our Recall article, Jacob Ivie and Bradley Podliska present three models of decisionmaking from the 19th-century western plains of the United States, using examples from the Battle of Little Bighorn and the Battle of the Rosebud.

And as you work through some of the pressing issues facing the joint force, we are here to help your ideas get a complete and full airing out. The only way we can change is to help each other to see the need to do so and then suggest a proper path to that new future. We need you to help be a good wingman and show us how to succeed. **JFQ**

—William T. Eliason,
Editor in Chief

Sailors aboard USS *Dwight D. Eisenhower* stand watch as ship, along with other ships of *Dwight D. Eisenhower* Carrier Strike Group, transit Strait of Hormuz, November 26, 2023; an Iranian drone came within 1,500 yards of USS *Dwight D. Eisenhower* as it conducted flight operations in international waters of Persian Gulf on November 28 (U.S. Navy/Janae Chambers)

When Does Gray Zone Confrontation End?
A Conceptual Analysis

By Lukas Milevski

The gray zone remains one of the most fashionable strategic concepts of the past few years in the United States, similar to hybrid warfare in Europe. It encapsulates a particular subset of international relations, in the process affecting the ideational distinction between war and peace.

Yet from its inception, the gray zone concept has come under intellectual fire. First, its conceptual soundness and historical novelty were contested.[1] Later criticism targeted gray zone thinking for diverging from classical and neoclassical strategic thinking based on the theories of Carl von Clausewitz.[2] The historical novelty and Clausewitz-deviation criticisms are not particularly sound. First, the better gray zone theorists always acknowledged that it was not a historical novelty but argued only that it would come to dominate the new character of conflict. Second, gray zone theory rejects, to some degree, the authority of Clausewitzian and neo-Clausewitzian

Lukas Milevski is an Assistant Professor at Leiden University and a Baltic Sea Fellow at the Foreign Policy Research Institute.

strategic theory. For gray zone advocates, consequently, recourse to the Prussian falls flat by default. Criticism targeting the conceptual soundness of the gray zone was stronger but was ultimately rather superficial in its analysis.

Lackluster criticism does not necessarily save the gray zone concept. For it to be meaningful, the gray zone must have a point at which it ends and turns into something else—political consequences. That is, gray zone activity must be able to lead to either success or failure. For the concept to be useful, it must contribute meaningfully to a theory of success, to the creation of a coherent logic that leads provisionally to victory—an attribute often forgotten in strategy-making.[3] Gray zone theorists recognize this. Michael Mazarr, for instance, has suggested that "gray zone campaigns would also seem to call for a new theory of conflict—a set of principles and theories of success in gray zone environments."[4]

This challenge has not yet been satisfactorily answered. Even when understood on its own terms, the concept itself inherently inhibits a satisfactory answer. To demonstrate, this article first discusses conceptual analysis, its components, and how to do it, before moving on to exploring the concept of gray zone conflict, which is followed by a discussion of the gray zone's conceptual depth and the implausibility of generating a gray zone theory of success. The bottom line of the gray zone is that there is no way out of it while respecting its own self-assumed rules. Mazarr recognized this, and his prescriptions avoid addressing the gray zone directly. But at this moment his suggestions appear equally inapt and implausible.

On Conceptual Analysis

Although conceptual analysis may sound remote from military concerns, it is as crucial to military thought as to any scholarly thinking because the foundation of each activity remains fundamentally similar: concepts that divide reality as we perceive it into defined and understandable chunks. Ideas are not necessarily right or wrong but rather more or less useful at interpreting the world around us. Gray zone theorists often wield this defense when the gray zone or similar ideas are criticized: Officials and theorists using these concepts "are merely trying to get a handle on what is going on, and believe that some encompassing category—gray, hybrid, or otherwise—can help us do it."[5] Scholarly conceptual analysis can get complex, but for present purposes it can be relatively simple, engaging with only three conceptual elements: definition, operationalization, and depth.

Concept definition and operationalization are mirror images of one another, the former abstract and the latter tangible. In academic literature, definition is often referred to as intension and operationalization as extension. *Intension* is the formal, abstract definition of a concept. *Extension* represents applicability of the concept to the real world, the set of physical objects or intangible but still perceivable relationships that the definition describes. First and foremost, the definition acts as a checklist: If a real-world phenomenon does not meet the features present in a concept's definition, then it cannot be an example of that concept. The relationship between definition and operationalization is therefore often inverse: the more definitional elements there are, the more features a real-world phenomenon must exhibit to be considered an example of that concept. Therefore, the more specific the definition, the fewer actual examples or instances of it will exist.

Conceptual depth, in contrast to definition, comprises all features that inherently accompany the definition of a concept but are not necessarily explicitly incorporated into the definition itself. In exploring what makes a concept good, John Gerring wrote of conceptual depth that

> *The larger purpose of concept formation is not simply to enhance the clarity of communication (by showing where, precisely, the borders between concepts are located), but also the efficiency of communication. We are looking for a way to group instances/characteristics that are commonly found together so that we can use the concept's label as shorthand for those instances/characteristics. The utility of a concept is enhanced by its ability to "bundle" characteristics. The greater the number of properties shared by the phenomena in the extension, the greater the depth of a concept.*[6]

Gerring wrote, however, from the perspective of creating concepts rather than of exploring existing concepts; his purpose was to bundle effectively rather than to unpack and explore an existing bundle. To explore existing conceptual depth is to consider how the various definitional attributes interact to create meaning that is hidden by the definitional attributes themselves. Yet hidden meaning affects strategic thinking when the concept is employed in strategic analysis.

Such hidden meanings are crucial to strategic analysis and subsequent practice because strategic theory is meant to inform action. Clausewitz, who is most convincing on the role of theory, argued that this informing quality is not manifested through principles of war or prescriptions for strategy, but essentially as instinct:

> *Knowledge must be so absorbed into the mind that it almost ceases to exist in a separate, objective way. . . . Continual change and the need to respond to it compels the commander to carry the whole intellectual apparatus of his knowledge within him. He must always be ready to bring forth the appropriate decision. By total assimilation with his mind and life, the commander's knowledge must be transformed into a genuine capability.*[7]

Strategy-relevant knowledge can be understood according to a triple-layered structure. At the most general and abstract layer are systemic knowledge and theory in which belongs, for example, much of Clausewitz's *On War* or much of the work of Colin Gray.[8] As an example, the operational level of war is a systemic-level concept; it affects the intellectual system by which we think about strategy. General, systemic knowledge allows its users to generate context-specific concepts to address ongoing phenomena in specific detail. From the operational level of war, the U.S. Army generated the specific concept and codified doctrine of AirLand Battle. Such concepts are then employed to construct specific theories of victory to overcome and defeat the presently identified challenge. Gray zone conflict should probably be most accurately understood as such a specific concept as it reflects specific challenges facing the United States, although it does have potentially troubling systemic implications regarding the boundaries of war and peace. As such, it should be a concept that can directly contribute to crafting a theory of victory.

Instinct plays a role in this process of concept generation and subsequent theory-building, particularly but not only in the context of generating tactical orders based on the theory of victory. Yet, in absorbing new ideas that appear fit for purpose, instinct also absorbs their hidden depths, which are not immediately apparent. If those depths are inappropriate, their absorption will lead to inapt ways of thinking about strategic or geopolitical challenges.

The Gray Zone and Its Conceptual Depths

Exploring the gray zone's elusive conceptual depths requires first establishing its definition and identifying other key features. Unfortunately, gray zone theorists seem never to have developed any concise definition but instead provide a list of characteristics. Mazarr, among the most sophisticated of the gray zone theorists, offers the following features:

- pursuing political objectives through cohesive, integrated campaigns
- employing mostly nonmilitary or nonkinetic tools
- striving to remain under key escalatory or red line thresholds to avoid outright, conventional conflict
- moving gradually toward objectives rather than seeking conclusive results in a specific period.[9]

When pushed by critics, Mazarr admitted that "[g]ray zone strategies can be hard to distinguish from aggressive versions of garden-variety diplomacy," but argued that what differentiated gray zone activities were "the coherence, intentionality, and urgency of these campaigns, which is why it makes sense to discuss the gray zone as a distinct approach to strategy."[10] Moreover, this whole concept sits within a much larger geopolitical context defined by rising powers that wish to revise the global order in some way, but supposedly without war. Nuclear weapons also contribute to the context for gray zone conflict as they increase the dangers of any escalation. Hal Brands has noted how gray zone conflicts reflect "some troubling weaknesses of the existing order," notably its vulnerability to this sort of gradualist change-making.[11]

An unrecognized feature of most hybrid and gray zone theory is that it can inadvertently reinforce the dichotomous, purportedly problematic war/peace distinction that such theory is meant to reform.[12] Nadia Schadlow, referring to a *Naval War College Review* article by Donald Stoker and Craig Whiteside,[13] discusses examples of Chinese gray zone activities:

> *How would* [Stoker and Whiteside] *interpret efforts by China to encourage Europeans to adopt Huawei's telecommunications hardware—a key part of an unfolding competition over control of information and data? It is not purely "peace," yet neither does it encompass the violence of war; however, it is strategically important. What would they call China's building of artificial islands in the South China Sea? This is an act without violence, but one that has shifted the status quo fundamentally. Is that an act of war? Or part of a competition designed to shift circumstances in Beijing's favor, without violence? Is that purely peaceful?*[14]

Yet the whole basis of Schadlow's perspective implicitly assumes that for something to be strategically important, it cannot be peaceful and might even be considered war. The problem appears to be not the dichotomy of war and peace as such but a specific vision of what peace entails.[15] The war and peace distinction is unrelated to assessments concerning the significance of international developments; something can be both peaceful and strategically important. The gray zone perspective seems to reflect the standard moral economy of Western concept creation. One wonders if Schadlow would consider U.S. pressure on the Dutch semiconductor company ASML not to do business with China or American encouragement of protestors on Maidan Nezalezhnosti (Independence Square) in Kyiv in 2013–2014 to be not purely peaceful.[16] At least some examples of gray zone theory unconsciously adopt problematic interpretations not only of war, but also of peace.

Characteristic of gray zone's conceptual features and context is the difficulty of determining its end, as Mazarr acknowledges: "[I]t can be difficult or impossible to define 'victory.' The goals of traditional warfare are typically clear, the definition of success or victory is self-evident, and once one side has 'won,' it is obvious to everyone. In gray zone campaigns, however, a clear concept of victory can be elusive."[17] He is mistaken about "traditional warfare"; the notion that its endings were typically unambiguous is historically and theoretically untenable, too often repeated by too many of both Clausewitz's disciples and critics. Nonetheless, the gray zone does exhibit a victory problem, which gray zone theorists have sought to resolve.

One group of authors has suggested that

> [w]*inning is perhaps better described as maintaining the U.S. Government's positional advantage, namely the ability to influence partners, populations, and threats toward achievement of our regional or strategic objectives. Specifically, this will mean retaining decision space, maximizing desirable strategic options, or simply denying an adversary a decisive positional advantage.*[18]

Mazarr has suggested that "gray zone campaigns are most likely to fail when they cannot sneak under the radar of the international system. The most important and ultimately effective response will therefore be to reaffirm and strengthen the norms, rules, and institutions of the international order." This assessment is based on the notion that gray zone activities are inherently self-defeating in the long term and that strengthening the international order would exacerbate this self-defeating

Russian soldiers with no insignia (so-called Little Green Men), at Belbek Airfield, as part of Russia's annexation of Crimea, in 2014 (Alamy/Stephen Foote)

characteristic—that is, addressing the gray zone challenge requires acting beyond the gray zone.[19] The explicit context for the gray zone is the world order and the stake of the revisionist powers in that order. According to Mazarr:

> *U.S. strategy must seek to multilateralize the international order, providing a more shared sense of ownership, and offering peaceful and constructive quasi-revisionists a greater say and stake in the system. The result would be a strategy of endorsing partial revisionism to discredit more radical varieties, and allow rising powers to shape events without investing in gray zone aggression.*[20]

Gray Zone's Conceptual Depths and a Theory of Success

The gray zone's conceptual depths have crucial implications for how strategists think while using the concept. These implications inhibit the development of an effective "blue" theory of success based on the gray zone concept and in response to hostile activities in the gray zone—although the gray zone does not actually represent a viable concept for a sustainable theory of success for the Russians or Chinese, either. Notably, for designing a blue theory of success, the gray zone is implicitly conceptualized as its own space in international relations, with its own rules. These rules essentially preclude the concept from being useful for military strategy, a point conceded implicitly by Mazarr as he also identified his own preferred theory of success beyond the gray zone. It is not possible to win within the gray zone, only outside of it. Yet this external theory of success runs up against "red" politics and Mazarr's own insight that it cannot provide the adversary with his own viable theory of success.

The entire concept of the gray zone instills a sense of place distinct from both war and peace. It is a bounded place with its own rules. By implication, to operate inside the gray zone requires following its perceived rules. The dangers of straying beyond it, particularly against China and Russia, are often highlighted: conventional war against major countries with sizable nuclear arsenals. The danger is too grave. This sense of place affects Western thinking in two ways: first, the West assumes it is a shared space; second, it encourages symmetrical thinking.

First, because the gray zone is a space, and spaces exist independently of their observers, we assume that all observers recognize the space. Thus, one frequent justification for gray zone thinking is that "precisely because our key competitors have developed a body of thinking related to the gray zone, there is reason enough to study these concepts. A central part of strategy—whether military or grand—is the need to understand 'the other,' the object of the strategy."[21] Although such words are sensible in principle, the gray zone and similar concepts fall flat in this regard, as Western strategy and defense debates—and attendant concept development—hardly pay attention to foreign military thinking in the first place, even when supposedly describing that same thinking. The result has been missteps, such as the fabrication of the Gerasimov Doctrine and the irony of the Russians importing the concept of hybrid warfare, *gibridnaya voyna*, from the West.[22] Given the comparatively less accessible character of Chinese, similar flaws likely exist in Western writings about Chinese strategy. Little Chinese foreign basis for a gray zone concept has been provided.

This is not to suggest that the Russians and Chinese do not have theories for geopolitically meaningful action short of war but that these usually appear still to be *peacetime* activities (depending on one's definition of peace), often with little or even no military substance. The Chinese "united front" aims to infiltrate and subvert Western societies and politics.[23] Furthermore, some Russian theory does distinguish between a zone of hostile subversion separating peace without hostility and outright war in a way that is reminiscent of the gray zone.[24] Ironically, given this similarity, the actual concept regularly applied to Russia—hybrid warfare—blends war and peace together in a way that the Russians do not. Yet the current hybrid and gray zone warfare debates are often little more than active mirror imaging: "This is how we would think about it if we were the Russians or the Chinese." These concepts do not necessarily bring the West any closer to understanding actual non-Western strategic thinking, particularly when the crucial aspect of that thinking is not that the Russians also conceptualize an interceding stage between peace and war but rather the logic of that stage, what activities it comprises and how they are performed, and on what grounds hostile subversion might escalate to outright war.

Second, through conceptualization as a space, the gray zone encourages symmetrical thinking—that the West must respond to gray zone activities through its own activity in the gray zone. Mazarr does warn against this: "The most fundamental response to this challenge is not to become tactically brilliant in the gray zone—it is to render the zone mostly moot, and take advantage of the inherent limitations and dilemmas involved in the employment of such strategies."[25] Brands similarly argues that the best way to address the gray zone is to remove ambiguity, to make it less gray and to make victim countries more resilient against subversion and nonmilitary pressure.[26] Mazarr's and Brands's real arena for countering the gray zone is the international order, yet most of the work done on the gray zone is more narrowly operational within the gray zone—that is, symmetrical. Some gray zone thinking may simply be out of necessity: the conceptual cat is out of the bag, and it remains the concept currently in use.[27]

Within this symmetrical strategic context, the assumed rules of the gray zone take hold and condition political and strategic behavior. Yet these guidelines to limit one's own military effort inhibit strategy and the ability to overcome the opponent's will to resist or to continue a gray zone campaign. Edward Luttwak identifies the very pinnacle of strategic performance as "the suspension, if only brief, if only partial, of the entire predicament of strategy."[28] The best strategies generate unanswerable asymmetries or somehow redefine the parameters of the conflict so that the adversary cannot respond effectively.[29] Operating *in* the gray zone against a gray zone actor does neither; the theory of success is already off to a poor start, a direction with which Mazarr sensibly disagreed.

Yet, as Mazarr acknowledges, revisionist powers such as Russia and China resort to gray zone means and methods because they cannot achieve their goals through the existing order. Western powers are unwilling to give up those things—political or legal principles, geopolitical or geoeconomic position, and so forth—that would be required for revisionists to achieve their goals. Yet the gray zone concept gives no suggestion as to why Russia or China would give up goals that they publicly identify as vital. For its part, the West is highly unlikely to give up much to the revisionists, either in terms of interests or principles. Revisionists' goals thus simply lie beyond the tolerance limits of the international order.

The zero-sum nature of the gray zone is crucial to the concept's utility for crafting a theory of success. Negotiation is not possible in a zero-sum contest. Each adversary identifies at the outset only two possible results: victory or defeat. Given the inability to either incorporate or accommodate the revisionists, coercion is required, but the assumed rules of the gray zone inhibit the West from overcoming both the opponent's powers of resistance and his will to resist—escalation is considered imprudent at best and impossible at worst, limiting the range of available responses.

The resulting contest is unbalanced despite its approximate symmetry. The gray zone aggressor advances a few salami slices at a time, altering physical realities with comparative ease by acting where or when the gray zone defender is not present and presenting a fait accompli that can be rolled back only by direct confrontation—that is, by plausibly, if not probably, dangerous escalation. The defender faces much greater difficulty preserving the physical situation, which requires active defense to deny the aggressor every inch, for an undefended inch can be lost. Such a policy is financially costly and prohibitively materially intensive. As a result, gray zone defenders generally seek to bring about behavioral change through legal arguments using military power (the freedom of navigation voyages through the South China Sea) or by punishing the aggressor and, at best, limiting his resources for future aggression (sanctions against Russia after 2014). Aggressors salami-slice; defenders seek to exhaust politically. Crucially for any gray zone theory of success, the conflict is one of endurance.

This extended duration is the product of three factors: the aggressor's care to avoid escalation while continuing to salami-slice; the defender's identical caution; and additionally, the defender's fundamental influence, of which caution is itself a product: limited political engagement. Thus, the issues at stake remain important enough for the West to demonstrate interest, become involved, and contest the outcome, but not important enough to escalate and resolve the situation. There are obvious reasons not to prefer the latter: Modern conventional warfare is costly, nuclear war is overly dangerous, and the issue would hardly be definitively resolved short of major regime change in the aggressor countries, all but certainly provoking nuclear war. As a result, gray zone confrontation is just a political

Taiwan Air Force F-16 monitors Chinese People's Liberation Army Air Force H-6 bomber as it passes near Taiwan airspace, February 10, 2020 (Taiwan Defense Ministry)

holding pattern, running the clock down because the issue can neither be solved nor abandoned.

Mazarr emphasizes the importance of endurance, arguing in boldface to "Make Sure Time Is on Your Side," although his subsequent suggestion was, in keeping with his preference for eschewing direct confrontation, "to set the conditions so that long-term social, political, and economic trends favor the United States, its allies and friends, and the stability of the rules-based order"—endurance outside, rather than inside, the gray zone.[30] His suggestion has much in common with George Kennan's notion of containment during the Cold War, which was premised on a basic theory of success emphasizing the degree to which its own internal contradictions would eventually result in its collapse. Although others twisted Kennan's logic, that essential logical chain remained intact to the end. It was a coherent theory of success reliant predominantly on the mere passage of time, although to many contemporary observers, it must have appeared as incredibly optimistic thinking.

Any gray zone theory of success must face the question of who gains greater advantage from an extended confrontation, in or out of the gray zone. Within the gray zone, time seems to benefit the aggressor more, as salami-slicing to change facts on the ground is generally slow. By contrast, the value of time for the defender is more likely to be negative: It enables the aggressor to continue changing physical reality, although this is likely to be true regardless of whether the defender sought to engage in gray zone confrontation or not. More time does not appear to give the defender any real advantage. Whereas the aggressor may have conquered or built a few more islands in the South China Sea and so advanced his cause, for example, for the defender the options and obstacles remain essentially the same. The only path to success is to imagine, as Kennan did and Mazarr does, that time will bring change sufficient to alter the revisionists' aims—change beyond the gray zone itself. The aggressor retains the initiative throughout the entire process.

The aggressor's constant initiative is crucial in the context of a key flaw of gray zone aggression, which appears to sustain this hope for change. The flaw is that, although it is straightforward to salami-slice territory, it does not necessarily work on political will and opinion. As time marched on after the invasions of Crimea and Donbas in 2014, Russia discovered the limits of subversion and nonmilitary pressure—the self-sabotaging nature of gray zone aggression that Mazarr identified. For Russia to attempt gradually to wear away the Ukrainian political will to join the West during a mostly frozen conflict post-2015 and expect results even by 2022 was a misjudgment. Ultimately, the will underpinning political behavior can be ground down only so far. Ukraine's choice to face West or turn back East is not a decision on a spectrum, but of kind: West or East. Such a decision is made in a single moment, not bit by bit, slice by slice. This is the fundamental limit of the gray zone concept even for aggressors: It is insufficiently decisive to lead to major political change. Russia's initial approach to dealing with Ukraine, purported to be a gray zone campaign, sabotaged its political ambitions in Ukraine in the longer term by divorcing from Ukraine the most pro-Russian territories in Crimea and Donbas.

People's Liberation Army Air Force sends Chinese H-6K bombers and other aircraft, including fighters, scouts, and tankers, to patrol islands and reefs, including Huangyan Dao, in South China Sea, undated (Xinhua/Alamy/Liu Rui)

Yet the result has not been a moderation of Russia's revisionist aims, as the gray zone theorists implicitly expect to be the result of the aggressor's gray zone failure, but instead an escalation to major war to fulfill them as Russia—or at least Vladimir Putin—ran out of political patience and perhaps foresaw increasingly limited opportunities to reverse Ukraine's trajectory in the future. As Mazarr suggests, gray zone aggression is not actually an effective theory of victory for the aggressor, unless victory is defined exclusively by conquest of territory. Yet presumably *because* Russia felt that time was on the side of the West, it became critical to escalate to get the desired result before it became impossible, thereby contradicting the fundamental assumption inherent in the gray zone concept that the aggressor fundamentally wishes to avoid war. The ironic result is that the defender's resilience within the gray zone may well lead not to peace and a reconciliation with the international order but to war and an ever-widening divergence from that order.

The situation is equally bleak for the defender. As a result of the way the concept is understood, direct confrontation in the gray zone is, if not self-defeating, then essentially futile. This suggests that the only way to beat the gray zone is not to fight in it—but not as Mazarr argued, by leveraging the international system, as this appears insufficient to alter major revisionist political goals. The answer instead appears to be unfortunately dangerous: escalation. Escalation by a defender may be the only way to escape the gray zone to achieve success. The gray zone aggressor, particularly if equipped with a reserve of nuclear weapons, poses a substantial escalation dilemma to the defender.

Yet by acting below what the West widely considers the threshold for war, gray zone aggressors reveal that among the responses they truly fear is precisely real, significant, applied military power. Moreover, they presumably consider the U.S. military threat to be credible. If neither were true, it would become more difficult (albeit not impossible) to explain why Russia or China would employ gray zone methods rather than outright seizure of what they want, to hold it behind a conventional and nuclear barricade. Gray zone aggressors pose an escalation dilemma to the defender, but the hypothetically escalating defender would reflect the hypothetical escalation dilemma back onto gray zone aggressors, not least because serious escalation reflects real political will and commitment to protect certain outcomes. The difference between the defender and the aggressor escalating to war is timing: Which side is ready, and which is unready?

Embarking on such a response to gray zone aggression—the only viable path to success—would clearly be a political, military, and strategic gamble. Of course, when faced with such a prospective course of action out of the gray zone, merely marking time within it appears quite an attractive policy option—and for good reason. And even if the passage of time generates aggressor frustration and even resultant massive military escalation, in the right circumstances this might still prove to be a mistake for the defender to exploit—as the West has been doing during Russia's reinvigorated invasion of Ukraine.

Conclusion

To be strategically useful, concepts should contribute in some way to the building of specific theories of success. Any concept that cannot do so is unlikely to be analytically or theoretically useful to practicing strategists; relying on such concepts may cause confusion and harm. However, such concepts are not totally unhelpful; they may possess high social utility within social and political dimensions of defense and strategy (focusing political attention and will, justifying budgets, and so forth).

The gray zone is one such concept. Within its very constitution it inhibits the creation of a theory of success that adheres to the assumed rules of the gray zone; instead, victory is achieved by those who *preempt* the gray zone through international resilience (Mazarr's preference even as an advocate of the concept) or escalate out of it. Nevertheless, the gray zone has been a highly fashionable concept within the U.S. defense establishment, undoubtedly because of its undeniably substantial social utility in focusing political and bureaucratic attention, will, and money on revisionist challenges to the United States and the international order it protects.

Antulio Echevarria posits that the gray zone concept is unlikely to be killed—it will eventually die its own natural death when supplanted by an even more fashionable concept—but we should still be able to qualify how we use this concept: to emphasize its social utility, its marketing value, rather than its negligible or even nonexistent strategic-analytical merit. The 2022 National Defense Strategy (NDS) mentioned the gray zone 12 times in its 80 pages, yet these mentions reflect the basic conceptual problems identified: Both threat vectors and the potential suite of useful instruments are identified, but there is no sense in the NDS of how the gray zone concept can contribute to an actual theory of success and enable the United States to succeed. The NDS promises a substantial amount of activity but can only weakly imply how and why this activity would produce success.[31] **JFQ**

Notes

[1] See the debate that occurred on *War on the Rocks*: Adam Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," *War on the Rocks*, December 15, 2015, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/; Adam Elkus, "Abandon All Hope, Ye Who Enter Here: You Cannot Save the Gray Zone Concept," *War on the Rocks*, December 30, 2015, https://warontherocks.com/2015/12/abandon-all-hope-ye-who-enter-here-you-cannot-save-the-gray-zone-concept/.

[2] Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking," *Naval War College Review* 73, no. 1 (Winter 2020), 13–48.

[3] On theories of success, see Frank G. Hoffman, "The Missing Element in Crafting National Strategy: A Theory of Success," *Joint Force Quarterly* 97 (2nd Quarter 2020), 55–64.

[4] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015), 103.

[5] Michael J. Mazarr, "The Strange Debates of Strategy," *War on the Rocks*, January 14, 2016, https://warontherocks.com/2016/01/the-strange-debates-of-strategy/.

[6] John Gerring, "What Makes a Concept Good? A Criterial Framework for Understanding Concept Formation in the Social Sciences," *Polity* 31, no. 3 (Spring 1999), 379–380.

[7] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 147.

[8] See, for example, Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010); Colin S. Gray, *The Future of Strategy* (Cambridge: Polity, 2015); and Colin S. Gray, *Theory of Strategy* (Oxford: Oxford University Press, 2018).

[9] Mazarr, *Mastering the Gray Zone*, 58.

[10] Michael J. Mazarr, "Struggle in the Gray Zone and World Order," *War on the Rocks*, December 22, 2015, https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/.

[11] Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/.

[12] I take Clausewitz's page one definition of *war* to be the best available definition: an act of violence to impose our will upon the enemy. Warfare is the conduct of war. See Chiara Libiseller and Lukas Milevski, "War and Peace: Reaffirming the Distinction," *Survival* 63, no. 1 (February–March 2021), 101–112.

[13] Stoker and Whiteside, "Blurred Lines."

[14] Nadia Schadlow, "It's a Gray, Gray World," *Naval War College Review* 73, no. 3 (Summer 2020), 140.

[15] This is a point that requires further exploration in a dedicated article.

[16] On the moral economy of another Western strategic concept, see Yves Winter, "The Asymmetric War Discourse and Its Moral Economies: A Critique," *International Theory* 3, no. 3 (2011), 488–514.

[17] Mazarr, *Mastering the Gray Zone*, 66.

[18] Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (4th Quarter 2016), 108.

[19] Mazarr, "Struggle in the Gray Zone and World Order."

[20] Ibid.

[21] Schadlow, "It's a Gray, Gray World," 141.

[22] See Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/; Ofer Fridman, *Russian "Hybrid Warfare": Resurgence and Politicisation* (London: Hurst & Company, 2018).

[23] June Teufel Dreyer, "A Weapon Without War: China's United Front Strategy," Foreign Policy Research Institute, February 6, 2018, https://www.fpri.org/article/2018/02/weapon-without-war-chinas-united-front-strategy/.

[24] See, for example, Vitaly Kabernik, "The Russian Military Perspective," in *Hybrid Conflicts and Information Warfare: New Labels, Old Politics*, ed. Ofer Fridman, Vitaly Kabernik, and James C. Pearce (Boulder, CO: Lynne Rienner, 2019), 43–65.

[25] Mazarr, *Mastering the Gray Zone*, 126.

[26] Brands, "Paradoxes of the Gray Zone."

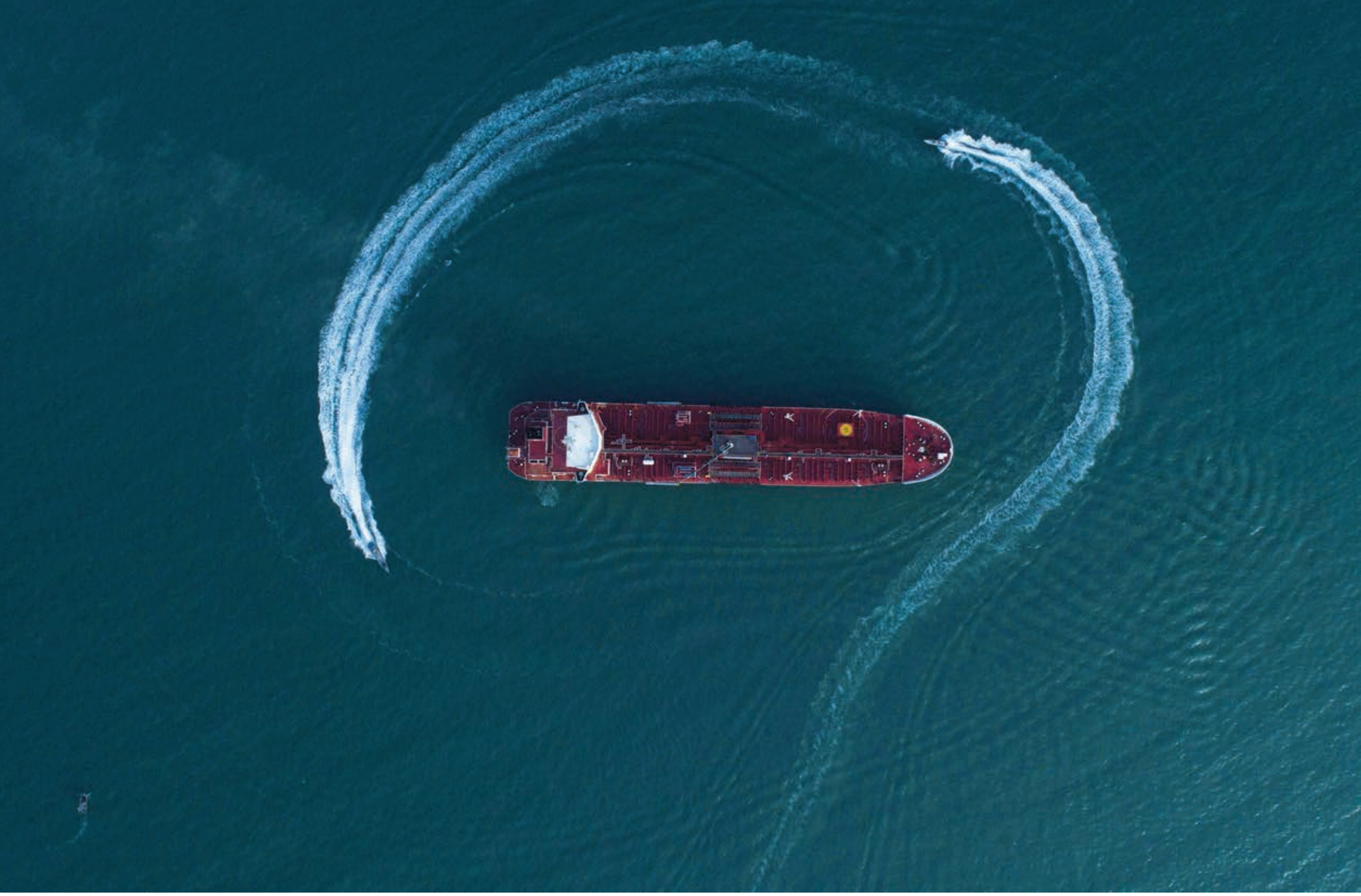
[27] Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy* (Carlisle, PA: U.S. Army War College Press, 2016), 4.

[28] Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press of Harvard University Press, 2001), 4.

[29] Lukas Milevski, "Asymmetry Is Strategy, Strategy Is Asymmetry," *Joint Force Quarterly* 75 (4th Quarter 2014), 77–83; see also Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005).

[30] Mazarr, *Mastering the Gray Zone*, 126.

[31] *2022 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2022). See also "The National Defense Strategy Shows the Pentagon's Increased Focus on the Gray Zone. Here's What That Means," Atlantic Council Hybrid Conflict Project, December 13, 2022, https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/the-national-defense-strategy-shows-the-pentagons-increased-focus-on-the-gray-zone-heres-what-that-means/.



Speedboats of Iran's Islamic Revolutionary Guard Corps surround British oil tanker *Stena Impero*, in Strait of Hormuz, July 19, 2019 (Imago/Alamy)

Position, Navigation, and Timing Weaponization in the Maritime Domain

Orientation in the Era of Great Systems Conflict

By Diane M. Zorri and Gary C. Kessler

Diane M. Zorri is an Assistant Professor of Security Studies at Embry-Riddle Aeronautical University and serves as a Nonresident Fellow in the Modern War Institute at West Point and Joint Special Operations University. Gary C. Kessler, CISSP, is a Nonresident Senior Fellow in the Cyber Statecraft Initiative at the Atlantic Council. He is President of Gary Kessler Associates, a consulting, research, and training company located in Ormond Beach, Florida, and a Principal Consultant at Fathom5, a maritime digital services company headquartered in Austin, Texas.

Deception, confusion, and targeting of weak points in modern warfare is as ubiquitous now as it was in the wars of antiquity.[1] Likewise, the incongruity between perception and reality has been explored for centuries. Understanding what is real is still a challenge for humankind. How does the human learn to "see" through the fog of deception? With the mind's ability to emphatically alter perceptions, modern society has become increasingly reliant on technology. Yet even technology can be deceptive, and, as Sun Tzu observed, "all warfare is based on deception."[2]

Strategists have long recognized that naval superiority and control of maritime assets are paramount in establishing global influence.[3] Alfred Thayer Mahan noted that although navies have an essential utility in safeguarding global trade and communications, a small naval force could overwhelm a much larger one by concentrating efforts on its adversary's key vulnerabilities. Consequently, when a country's maritime assets come under attack, it may have far-reaching geopolitical, military, and economic implications. The sinking of the USS *Maine* (1898) and RMS *Lusitania* (1915), as well as the attacks on the USS *Maddox* and USS *Turner Joy* (1964), precipitated major conflicts and sustained military campaigns. While the U.S. Navy remains the largest and most expeditionary force in the world, smaller forces, malign powers, and irregular adversaries are disrupting maritime transit and naval assets using new and innovative techniques. These techniques often involve a "system of systems" approach, where malign actors confront adversaries through critical components of operational systems.[4] Two of the most persistent threats to maritime security and superiority in the great systems conflicts of the 21st century stem from vulnerabilities in two of the technologies that enable position information, navigation, timing, and situational awareness: the Global Positioning System (GPS) and the Automatic Identification System (AIS).[5]

The maritime domain is often overlooked in its criticality to U.S. national security. Ninety percent of U.S. import and export trade is via ship, and the Maritime Transportation System (MTS) contributes $5.4 trillion to the national economy, representing about 25 percent of the U.S. national gross domestic product (GDP). The MTS is an expansive network of navigable channels, ports, locks, marine terminals, marinas, and seaways that facilitates this trade. Like the MTS but on a global scale, the global maritime transportation network (GMTN)—an arrangement of seaports, waterways, ports, and terminals that accounts for over 70 percent of the value of global trade and nearly 90 percent of its volume—facilitates the global economy. These systems are complex and interdependent, and much like other facets of critical infrastructure, their constituent parts are often undervalued in terms of being integral components of the global economy and strategic security.[6] It is no exaggeration to suggest that the MTS is integral to our food, energy, financial, and national security, as well as our projection of military power around the globe.[7]

GPS

The world's MTS relies on the four major global navigation satellite systems (GNSS)—BeiDou (China), Galileo (European Union), GLONASS (Russia), and GPS (United States)—for navigation, routing, and situational awareness at sea. A GNSS provides position, navigation, and timing (PNT) services that are used not only for land-, sea-, and air-based navigation but also for the precision timing necessary for critical infrastructures. The importance of timing cannot be overemphasized; if GPS timing signals fail or are severely impaired, there will be widespread failure of telecommunications, financial services, transportation, and power distribution networks, to name just a few.

GPS can offer positioning information accurate to within 3 feet of a receiver's actual location.[8] While such precision might not be necessary on the high seas (so-called blue water), accurate PNT is essential in littoral zones (brown water) and while traversing narrow chokepoints and critical nodes such as the Strait of Hormuz, Strait of Malacca, Panama Canal, Bosporus Strait, and Suez Canal.[9] GPS is widely recognized as the best GNSS in the world in terms of accuracy, precision, and reliability and, for this reason, is the most widely used system in the world.[10] GPS, however, suffers from three vulnerabilities: jamming, spoofing, and total system failure.

Jamming refers to a receiver being unable to detect a legitimate GPS signal due to interference from nearby radio transmissions. A GPS signal is transmitted from a satellite—at an altitude of 12,550 miles—at approximately 50 watts of power. The signal arrives at the Earth's surface, however, at a fraction of a milliwatt. Thus, a malign actor may broadcast signals on the GPS frequencies at even a few watts of power and overwhelm the ability of a receiver to acquire necessary PNT information from the GPS signal.[11]

GPS jamming is not a new phenomenon. While initially developed for the military, inexpensive GPS jammers have been available to the public—albeit illegal to use—for well over a decade. One of the earliest widely publicized examples of this activity involved a person fined in 2013 for using a GPS jammer in the proximity of Newark Liberty International Airport and interfering with flight operations. Rampant GPS jamming activities are taking place around the world, most notably at airports, with Norway being particularly affected. Moreover, China, North Korea, and Russia each have long histories of efforts to jam or otherwise neutralize the GNSS of other countries.[12]

GPS *spoofing* causes a receiver to report its location at one place when it is in another place. In 2012, a team from the University of Texas at Austin first demonstrated spoofing to the Department of Homeland Security by spoofing GPS signals to a drone, causing it to lose awareness of its proper altitude. In June 2013, the same team was able to spoof the location of the *White Rose of Drachs*, an $80 million, 213-foot superyacht, causing it to change course in the middle of the Mediterranean Sea.[13] GPS spoofing is not limited to laboratory conditions. The first large-scale public case of GPS spoofing in the MTS was in June 2017. M/V *Atria* was anchored in the Black Sea off the Russian port of Novorossiysk, but its GPS reported its location as Gelendzhik Airport, 20 nautical miles away. The 37.5-ton tanker was not alone; the receivers on at least two dozen other vessels placed them in the same location.[14]

The *Atria* incident was neither an isolated event nor even the first such spoofing incident.[15] In 2019, the Center for Advanced Defense Studies released a report describing nearly 9,900 incidents of GPS spoofing incidents in the Black Sea, Crimea, the Russian Federation, Syria, and other locations as far back as 2016, all linked to the Russian military.[16] In 2020, investigative journalists reported that a German research vessel detected GPS spoofing and jamming events in many sites on its worldwide voyage in 2017 and 2018.[17]

Destruction of the entire GPS system is, of course, the ultimate vulnerability. GPS employs a constellation of more than 32 satellites, 29 of which are in use at any one time—a minimum of 24 are required for the system to operate. By design, GPS is resilient to "natural" failures; if one satellite suffers a failure, it is moved out of position and a replacement takes over. Yet Russia and China have both demonstrated "satellite killer" capability, and, since the spring of 2021, Russian President Vladimir Putin has repeatedly threatened to shoot down many, or all, GPS satellites.[18] GPS has no resiliency against such a systemic failure.

The vulnerabilities of and threats to GPS are not merely issues for the maritime community but affect all aspects of modern society. There is not a concentrated effort to supplement or augment GPS in the near term. While GPS is managed by the U.S. Space Force, it is both a military and a civilian asset, so something bigger than a military solution is required.[19] The Russian invasion of Ukraine in February 2022 highlighted both the necessity of an assured PNT system and the requirement for augmentation.[20]

AIS

GPS and other GNSS facilitate the Automatic Identification System, the global system used by ships and maritime authorities to maintain situational awareness of local vessel traffic. AIS data, as aggregated by several sites worldwide, has evolved to provide a historical log of a ship's movement over time. AIS is important for tracking shipping routes, basic industry intelligence, and awareness about shipping in general. AIS was designed in the 1990s, primarily in response to the oil spill that followed the grounding of *Exxon Valdez* in 1989. Required in the 2002 Safety of Life at Sea (SOLAS) Convention, AIS has several well-known security vulnerabilities, including the lack of sender authentication, message timestamps, data validity verification, and data content integrity. Although all large U.S. military vessels have AIS transceivers, most transceivers are not broadcasting most of the time because of the warship exemption in the SOLAS requirements.[21]

One early example of a combination of GPS and AIS spoofing is the Iranian seizure of the United Kingdom (UK)–flagged tanker *Stena Impero*. Steaming through the Strait of Hormuz in international waters in July 2019, *Stena Impero* suddenly turned north and entered Iranian territorial waters, where it was promptly seized by patrol boats of the Iranian navy. This incident was likely in retaliation for the British seizure of an Iranian vessel earlier in the year due to suspected violations of European Union sanctions.[22]

The episodes of spoofing continued and morphed into more powerful displays of disruption. In July 2019, the U.S.-flagged M/V *Manukai* reported a series of false GPS and AIS readings at the Port of Shanghai.[23] Unlike previous spoofing events that made a vessel believe that it was in the wrong place, the *Manukai* saw target vessels that appeared to be jumping around. Further analysis of many events that occurred in the area made it appear that the spoofed locations appeared in circles.[24] Dubbed "crop circles," similar spoofing was found in other locations, including Tehran. In all these cases, the vessels were in the proximity of the spoofing. Later analysis showed circle spoofing occurring around Point Reyes (just north of San Francisco), where the spoofed vessels were as far as 10,000 miles away from the area.[25]

The Port of Shanghai and subsequent circle spoofing incidents have escalated from spoofing vessels within the proximity of the spoofer to where ships can be anywhere on the globe relative to the spoofed location. China is one of the chief suspects in these circle spoofing events. They have long been suspected of AIS spoofing to hide their fishing fleets that are involved in illegal, unreported, or unregulated (IUU) fishing by showing them to be hundreds or thousands of miles away from their actual locations.

These episodes of AIS spoofing have been perpetrated for many purposes, including demonstrations of capability; masking IUU fishing, smuggling, and other illegal activities; and identity laundering to avoid detection, sanctions, or inspections.[26] Widespread spoofing of warships, however, represents an even more dangerous level of escalation, exacerbated by the fact that warships do not always routinely broadcast AIS information. As an example, AIS data showed the HMS *Queen Elizabeth* and five escort vessels steaming toward the Irish Sea in September 2020, while contemporaneous satellite imagery showed an empty ocean in their supposed location. In fact, not only were the six vessels not where their AIS track put them, but they were not even together at the time—and likely not even actually broadcasting AIS messages.[27]

In this context—and that of subsequent events in the area—the AIS spoofing of North Atlantic Treaty Organization (NATO) vessels in the Black Sea in June 2021 takes on an entirely different significance. Prior to a scheduled exercise late that month, two NATO warships, HMS *Defender* (UK) and HNLMS *Evertsen* (the Netherlands), arrived in Odesa (Ukraine) on the afternoon of June 18. AIS tracking data showed both ships traveling directly to Sevastopol (Crimea) later that night, positioned within 2 nautical miles of the port housing the Russian Black Sea fleet command. YouTube video, live webcam, and other evidence, however, showed that neither vessel left its dock. Because of the contested sovereignty of Crimea and the presence of the headquarters of the Russian Black Sea Fleet in Sevastopol, the unannounced approach of NATO vessels into what Russia claims are its territorial waters could well be described as an act of provocation.[28] Indeed, AIS tracks showed the USS *Ross* near Crimea about 10 days later, although live webcams showed it at dock in Odesa.[29]

The 2021 Black Sea incident was part of a much larger pattern of the spoofing of AIS tracks of warships from many nations over the last several years.[30] (As a demonstration of the ease with which AIS spoofing can be accomplished, one of the authors of this article showed the spoofed track of Russian guided-missile cruiser *Moskva* entering Port Canaveral on the east coast of Florida [see figure 1] at DEFCON's Hack the Ship Village in August 2021.[31])

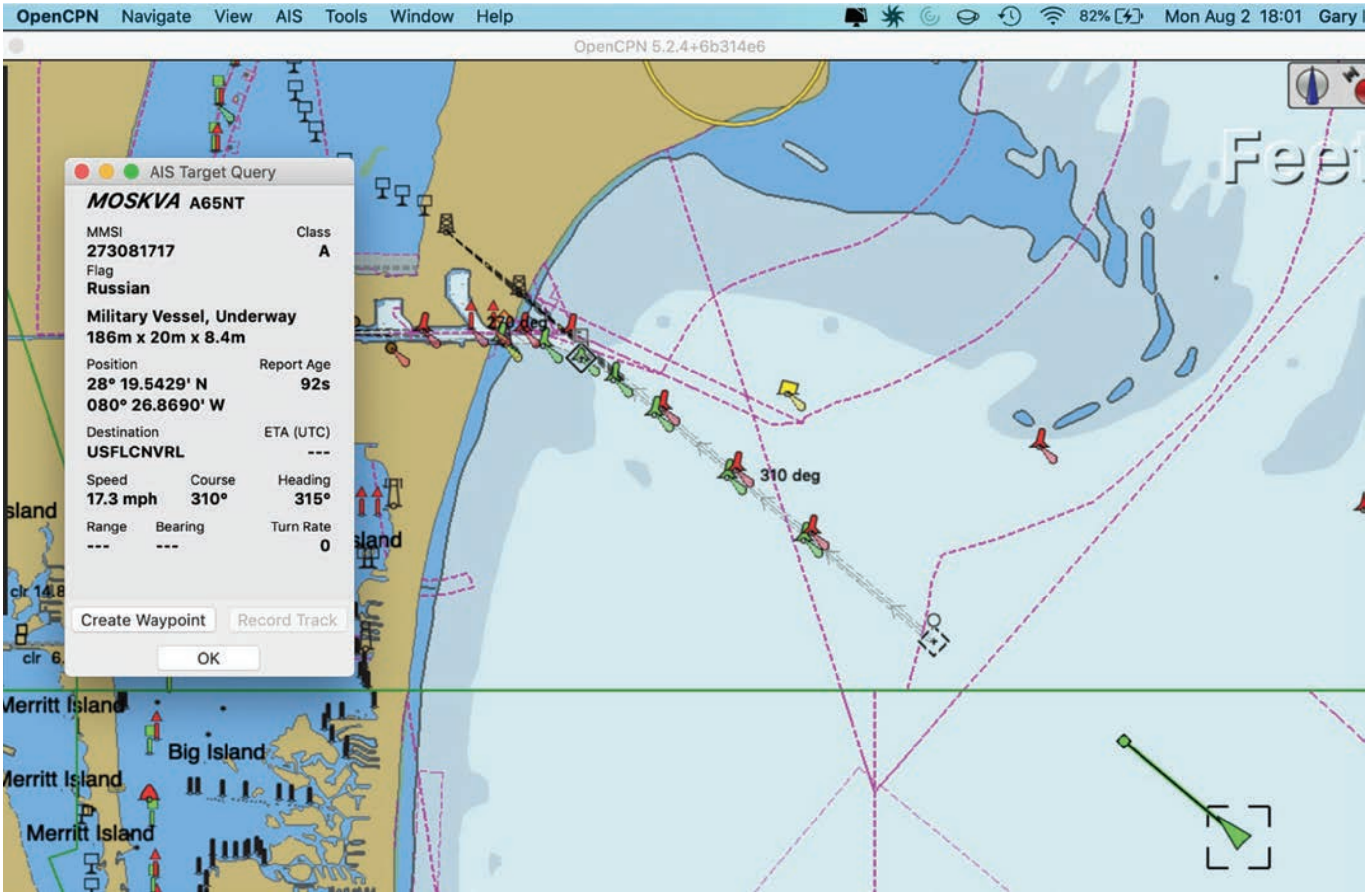
Geopolitical Risks and Implications

Historical Parallels. The 2021 Black Sea incident appears to be the pre-staging of history. The most likely source of the spoofing of NATO vessels is Russia, which was able to engage in saber-rattling rhetoric in the aftermath of the events. Although most of the world understood that the tracks were bogus, the Russian people likely believed the evidence of NATO aggression. From Putin's standpoint, his domestic audience—not the rest of the world—is the only audience that needs to be convinced of anything.

It is uncertain whether the spoof of the NATO vessels was a test of capability or if it was intended as a pretext to war. If it was the latter, it would not be the first time that false electronic signals at sea have provided a rationale for armed conflict. Consider the object lesson of the Gulf of Tonkin incidents. On August 2, 1964, the USS *Maddox* came under attack by three North Vietnamese patrol boats. At the end of the skirmish, all the attacking patrol boats had been damaged, 10 North Vietnamese sailors were killed or wounded, and one bullet hole was found in the *Maddox*. This was the first Gulf of Tonkin incident. Two days later, the *Maddox* and USS *Turner Joy* detected approaching North Vietnamese patrol boats on radar. Seeing what they thought were torpedo tracks on radar and sonar, the vessels fired on the patrol boats, even though neither ship nor any U.S. naval aircraft made visual contact with the attackers.[32] This was the second Gulf of Tonkin incident, and the precipitating rationale for Congress to pass the Gulf of Tonkin Resolution, escalating the mission of U.S. forces in Vietnam.[33]

The second Gulf of Tonkin incident, however, never occurred. While there might well have been vessels around the radar's report, there were no attacking patrol boats, and there were no torpedoes. Misinterpreted and conflicting signals intelligence from both radar and sonar caused a response when there was, in fact, no stimulus. Yet in a rush to judgment—one that was politically popular and seemed to be consistent with enemy actions of just 2 days earlier—the signals intelligence (SIGINT) was not scrutinized, and contradictions

Figure. Spoofed AIS Track of *Moskva* Near Port Canaveral, Florida, August 2021



AIS Target Query

MOSKVA A65NT

MMSI: 273081717
Class: A
Flag: Russian

Military Vessel, Underway
186m x 20m x 8.4m

Position: 28° 19.5429' N 080° 26.8690' W
Report Age: 92s

Destination: USFLCNVRL
ETA (UTC): ---

Speed: 17.3 mph
Course: 310°
Heading: 315°

Range: ---
Bearing: ---
Turn Rate: 0

Ships from Standing NATO Maritime Group 2, including Italian Navy ITS *Alpino*, USS *Harry S. Truman*, and USS *Cole*, sail in formation in Mediterranean Sea, July 24, 2022 (U.S. Navy/Crayton Agnew)

that were known at the time were not investigated.[34] An attack—whether real or imagined—was consistent with the narrative and political winds of the day.

Implications and Countermeasures. There is great danger when the warships of rival nations come into proximity to one another. When operators can deliberately alter SIGINT and navigation signals to skew the truth—or the perception of the truth—the space is even more dangerous; intentional disruptions to these systems are provocative and have far-reaching consequences. Disrupting GPS and other GNSS creates navigational uncertainty, delays, and inefficiency in the supply chain. The disruptions can also cause accidents in littoral and near-coastal waters, narrow straits, and international chokepoints where ships operate with a small margin for error. False AIS tracks can support virulent narratives, countering the interests of U.S. allies and partners. Moreover, adversaries can spoof AIS to masquerade as a much larger force or change a ship's navigation history. While cyber attacks have not yet invoked a collective defense response or triggered Article

5 of the NATO treaty, the second- and third-order effects of these disturbances are incalculable.[35] Moreover, during each incident the U.S. Navy must quickly recognize the threats, orient its decisionmaking, and decide a response.

Given the ease of spoofing GPS and AIS signals, we are in a particularly dangerous environment. Any adversary government—whether China, Iran, North Korea, Russia, or others—could easily enter entirely fake tracks of vessel movements into the historical record, in real time. Although some might debate whether attacks on GPS and AIS are *cyber* in their nature, those arguments miss the point. The term *cybersecurity* is a misnomer; what we must focus on is protecting the confidentiality, integrity, availability, authenticity, utility, and possession of information and other necessary data.[36] From that perspective, attacks on GPS and AIS clearly affect multiple characteristics of navigational and situational awareness information.

Maritime cybersecurity is particularly pertinent today given Russia's invasion

Sailors assigned to USS *Zumwalt* participate in simulated ship transit while attending Bridge Resource Management course at Navigation, Seamanship, and Shiphandling Trainer on Naval Base San Diego, March 10, 2023 (U.S. Navy/Kevin C. Leitner)

of Ukraine. Ostensibly, one of Russia's pretexts for the war is the encroachment of NATO on Russia's borders.[37] Part of the demonstration of Alliance aggression could well be the spoofing of NATO vessels in June 2021. There is also significant evidence that Russia is using attacks on GPS in the war against Ukraine, targeting aerial, artillery, and other military systems, as well as communications systems (many of which rely on GNSS for timing).[38] Reportedly, Russian jamming has at times been so intense that it has interfered with Russia's own systems. When it comes to navigation, Russia has access to the Chayka terrestrial electronic navigation system as a backup to GLONASS and other GNSS.[39]

Now, most of the GPS jamming/spoofing mitigation strategies are short-term improvisations. Many commercial GNSS receivers, for example, can detect when an incoming signal on the primary constellation appears to be bogus. In some cases, the receiver can switch to an alternate GNSS constellation. There is, however, no backup available or augmentation capability in place for GPS. Prior to the widespread availability and use of GPS, the United States and international maritime community relied on the Long-Range Navigation (LORAN) terrestrial-based navigation system. The Department of Homeland Security decommissioned LORAN in 2010, leaving no maritime backup to GPS.[40] Indeed, today many mariners do not know how to use LORAN devices or understand LORAN markings on a chart. In 2018, the Trump administration mandated that the Secretary of Transportation establish a backup to GPS via a terrestrial-based timing system,[41] yet no work has commenced on the proposed replacement system, enhanced LORAN (known as eLORAN).[42] Another potential alternative to satellite-based position, navigation, and timing is the use of quantum sensors for positioning, yet researchers have not fully realized this capability. Likewise, while there have been several proposals to secure AIS, the international standards bodies have not been consistent in their planning or execution.[43]

Conclusion

The jamming and spoofing of GPS and AIS information has escalated in the last half-dozen years from simple demonstrations of capability to truly dangerous situations where misperceptions could ignite a major conflict. The attack surface is becoming increasingly ubiquitous and strikes on military assets can be staged via nonmilitary vectors.[44] The U.S. defense community can mitigate the vulnerabilities in its systems in several ways. First, training and awareness can make both military and commercial mariners aware of the frailties of the systems. Maritime operators and bridge officers should have knowledge of the information and operational technology systems aboard their ships and the myriad ways in which they are interconnected and how they interact. Information security–aware officers as well as shipboard detection systems should be integrated into maritime personnel and management systems. Navigation and bridge personnel must be able to determine when the information displayed by the automated systems is suspect and must have independent means of validating those systems. In addition, celestial navigation techniques and the science of inertial and hyperbolic systems need to be integrated into the curricula of maritime practitioners. Furthermore, maritime naval exercises need to include scenarios where GNSS and AIS have been disrupted by enemy forces and test how practitioners would respond without current technology. Exercises should also integrate opportunities that test the innovative capacity of cyber defenders as well as their ability to proactively target the enemy.

Next, lawmakers and funding agencies must be convinced that if the vulnerabilities in GPS and AIS are not addressed in the near term, the threat to national security is plausible and potentially cataclysmic. This onus lies on all PNT stakeholders, whether they are in the military, government, or commercial sector. Both the Chinese and the Russians use a terrestrial-based PNT system to augment their GNSS systems, giving them a significant strategic advantage over the United States.[45] Instead of recommending the short-term revival of LORAN as reserve capability, the National Space–based PNT Advisory Board has developed a strategy of toughening and modernizing the current GPS systems until non–GNSS PNT systems, like those that use quantum sensing, are widely available.[46] Another solution would be to integrate the National Aeronautics and Space Administration’s Jet Propulsion Laboratory’s Global Differential GPS (GDGPS) across the national security entities and critical infrastructure of the United States. GDGPS tracks data from all GNSS constellations and offers corrections and real-time accuracy for positioning applications.[47] Yet no single entity within the U.S. Government has been given the authority to fully implement a PNT augmentation capability or

U.S. Navy Quartermaster 3rd Class Hailey Pardo shoots sunlines with sextant aboard USS *Chung-Hoon*, Pacific Ocean, October 8, 2022 (U.S. Navy/Kenneth Lagadi) oversee an integrated PNT strategy. The full integration of the GDGPS system across the national security architecture would require strategic guidance and funding. Moreover, to compete with China, which many experts have begun to recognize as a global leader in comprehensive PNT capability, the United States needs to adopt a long-range strategic plan for PNT at the national level.[48] This plan should recognize the criticality of PNT to national security and holistically work to improve all PNT capabilities (that is, low-orbit satellites, space-based satellites, terrestrial navigation, inertial navigation, quantum sensing, LORAN, and celestial navigation) as an integral system of systems.

Alternatively, AIS security solutions are highly likely to yield positive gains to commercial industries. Competitive bids for AIS systems should integrate security measures, such as public-key or asymmetric cryptography, digital signatures, or a combination of the identity-based authentication that is commonplace in commercial applications, computers, and on mobile phones.[49] Yet securing AIS might be an even harder problem to solve because it demands international agreement within two United Nations organizations—the International Maritime Organization is responsible for SOLAS and the International Telecommunication Union for the AIS over-the-air protocol.[50] Mitigating this challenge will require a clear vision and proactive leadership.

Because of the grave danger that GPS and AIS weaponization entails, it is essential that policymakers and maritime operators understand not only the risks and implications of these threats, but also the mitigation techniques and countermeasures that add resilience to the warfighter. Moreover, the U.S. Government needs to address the significant advantage that our adversaries have developed in PNT resilience and augmentation. The redundancies and security initiatives may be costly, yet both PNT resilience and augmentation and AIS security measures are vital for protecting our nation's critical assets and mitigating a future conflict. **JFQ**

The authors gratefully acknowledge the support of the Naval War College and feedback from our fellow participants at the War College's Cyber and Innovation Policy Institute 2022 Summer Workshop on Maritime Cybersecurity.

Notes

[1] Sun Tzu, *The Art of War* (New York: Simon & Schuster, 2004).

[2] Ibid.

[3] Alfred T. Mahan, *The Influence of Seapower Upon History, 1660–1783*, 12th ed. (Boston: Little, Brown and Company, 2004), 12–16.

[4] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

[5] The term *great systems conflict* is attributed to Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era: Coalescing Against Cyber, Pandemic, and Adversary Threats," *The Cyber Defense Review* 6, no. 2 (Spring 2021), https://cyberdefensereview.army.mil/Portals/6/Documents/2021_spring_cdr/05_Demchak-CDR_V6N2_Spring_2021.pdf?ver=fpA19JdBy-n6fRbxSh8paA%3D%3D.

[6] *Cyber Strategic Outlook: The United States Coast Guard's Vision to Protect and Operate in Cyberspace* (Washington, DC: U.S. Coast Guard, August 2021), https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf.

[7] David Alderson, Daniel Funk, and Ralucca Gera, "Analysis of the Global Maritime Transportation System as a Layered Network," *Journal of Transportation Security*, November 28, 2019, 1–35, https://calhoun.nps.edu/handle/10945/25530; Jason Ileto, "Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition," *Modern War Institute*, May 10, 2022, https://mwi.usma.edu/cyber-at-sea-protecting-strategic-sealift-in-the-age-of-strategic-competition/; Gary C. Kessler and Steven D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers*, 2nd ed. (Kindle Direct Publishing, September 2022), https://www.maritimecybersecuritybook.com/.

[8] Pratap Misra and Per Enge, *Global Positioning System: Signals, Measurements, and Performance*, rev. 2nd ed. (Lincoln, MA: Ganga-Jamuna Press, 2021).

[9] Gary C. Kessler and Diane M. Zorri, *Cross Domain IW Threats to SOF Maritime Missions: Implications for U.S. SOF* (MacDill Air Force Base, FL: Joint Special Operations University Press, 2021), https://commons.erau.edu/cgi/viewcontent.cgi?article=2765&context=publication.

[10] Bill Bostock, "Downed Russian Fighter Jets Are Being Found With Basic GPS 'Taped to the Dashboards,' UK Defense Minister Says," *Business Insider*, May 10, 2022, https://www.businessinsider.com/russia-su34-jets-basic-gps-receivers-taped-to-dashboards-uk-2022-5.

[11] Tom Nardi, "Teardown: Mini GPS Jammer," *Hackaday*, September 8, 2020, https://hackaday.com /2020/09/08/teardown-mini-gps-jammer/.

[12] Tegg Westbrook, "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare," *Journal of Strategic Security* 12, no. 2 (2019), 1–16, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1720&context=jss.

[13] Mark L. Psiaki, Todd E. Humphreys, and Brian A. Stauffer, "Attackers Can Spoof Navigation Signals Without Our Knowledge. Here's How to Fight Back GPS Lies," *IEEE Spectrum* 53, no. 8 (August 2016), 26–53.

[14] Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" *The Maritime Executive*, July 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

[15] Westbrook, "The Global Positioning System and Military Jamming."

[16] "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," Center for Advanced Defense Studies (C4ADS), March 26, 2019, https://c4ads.org/reports/above-us-only-stars/.

[17] Katherine Dunn, "The Long Ocean Voyage That Helped Find the Flaws in GPS," *Fortune*, January 24, 2020, https://fortune.com/2020/01/24/gps-disruption-test-voyage/.

[18] Dana A. Goward and John Garamendi, "Putin Is Holding GPS Hostage. Here's How to Get It Back," *Defense News*, April 12, 2022, https://www.defensenews.com/opinion/2022/04/12/putin-is-holding-gps-hostage-heres-how-to-get-it-back/.

[19] Dana A. Goward, "Get the Bullseye Off GPS," *Space News*, April 19, 2022, https://spacenews.com/op-ed-get-the-bullseye-off-gps/.

[20] Olivier Chapuis, "En guerre en Ukraine, la Russie brouille la navigation par satellites et utilise le système Loran" [At war in Ukraine, Russia jams satellite navigation and uses the Loran system], *Voiles et Voiliers*, March 19, 2022, https://voilesetvoiliers.ouest-france.fr/equipement-entretien/electronique-embarquee/gps/en-guerre-en-ukraine-la-russie-brouille-la-navigation-par-satellites-et-utilise-le-systeme-loran-efd085fa-a6ac-11ec-969a-2a6df02632f3; Brian G. Chow and Brandon W. Kelley, "Russian Invasion of Ukraine Reinforces the Urgency of Fixing U.S. Satellite Vulnerability by 2027," *Space News*, March 8, 2022, https://spacenews.com /op-ed-russian-invasion-of-ukraine-reinforces-the-urgency-of-fixing-u-s-satellite-vulnerability-by-2027/.

[21] Kessler and Shepard, *Maritime Cybersecurity.*

[22] Michelle W. Bockmann, "Seized UK Tanker Likely 'Spoofed' by Iran," *Lloyd's List*, August 16, 2019, https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran.

[23] Mark Harris, "Phantom Warships Are Courting Chaos in Conflict Zones," *Wired*, July 29, 2021, https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/.

[24] "Shanghai GPS Spoofing," video, 0:42, C4ADS, 2019, for download, https://drive.google.com/file/d/1dTWu7H9JjRyN0uQPZ9HwiUzCFd7cd5pL/view.

[25] Bjorn Bergman, "AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco," *Sky Truth*, May 26, 2020, https://skytruth.org/2020/05/ais-ship-tracking-data-shows-false-vessel-tracks-circling-above-point-reyes-near-san-francisco/.

[26] James R. Watson and A. John Woodill, "Anticipating Illegal Maritime Activities From Anomalous Multiscale Fleet Behaviors," *Arxiv*, October 15, 2019, https://arxiv.org/pdf/1910.05424.pdf.

[27] Harris, "Phantom Warships Are Courting Chaos in Conflict Zones."

[28] H.I. Sutton, "Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base," *USNI News*, June 21, 2021, https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base.

[29] Yoruk Isik, "And . . . All Fake Like HMS Defender Incident. USS Ross Is in Odesa's Cabotage Harbor!" *Twitter*, June 29, 2021, https://twitter.com/yorukisik/status/1409992626477191175.

[30] Harris, "Phantom Warships Are Courting Chaos in Conflict Zones."

[31] Gary C. Kessler, "AIS Spoof of a Warship," video, 2:13, August 22, 2021, https://www.garykessler.net/gck/202108_MOSKVA_spoof.mp4. The *Moskva* sunk in the Black Sea during the Russian invasion of Ukraine in April 2022. The DEFCON hacker convention regularly hosts mini-conferences titled "Hack the Sea" or "Hack the Village," where participants in the information and security community are invited to partake in experiential learning on how to protect cyber assets.

[32] Robert J. Hanyok, "Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2–4 August 1964," *Cryptologic Quarterly* 19/20 (Winter 2000/Spring 2001), 4–10, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB132/relea00012.pdf.

[33] Dale Andradé and Kenneth Conboy, "The Secret Side of the Tonkin Gulf Incident," *Naval History Magazine* 13, no. 4 (August 1999), https://www.usni.org/magazines/naval-history-magazine/1999/august/secret-side-tonkin-gulf-incident.

[34] Hanyok, "Skunks, Bogies, Silent Hounds, and the Flying Fish."

[35] Cassia Sari, "Cyberattacks Can Invoke NATO Defence Clause," *The Organization for World Peace*, April 25, 2022, https://theowp.org/cyberattacks-can-invoke-nato-defence-clause/.

[36] Donn B. Parker, "Toward a New Framework for Information Security?" in *Computer Security Handbook*, 6th ed., ed. Seymour Bosworth, Michel E. Kabay, and Eric Whyne (Hoboken, NJ: John Wiley & Sons, Inc., 2015).

[37] Michael Klipstein and Tinatin Japaridze, "Collective Cyber Defence and Attack: NATO's Article 5 After the Ukraine Conflict," *European Leadership Network*, May 16, 2022, https://www.europeanleadershipnetwork.org/commentary/collective-cyber-defence-and-attack-natos-article-5-after-the-ukraine-conflict/.

[38] Jake Thomas, "'They're Jamming Everything': Putin's Electronic Warfare Turns Tide of War," *Newsweek*, June 3, 2022, https://www.newsweek.com/theyre-jamming-everything-putins-electronic-warfare-turns-tide-war-1712784.

[39] Chapuis, "En guerre en Ukraine, la Russie brouille la navigation par satellites et utilise le système Loran."

[40] *Terminations, Reductions, and Savings: Budget of the U.S. Government, Fiscal Year 2010* (Washington, DC: Office of Management and Budget, 2009), https://www.govinfo.gov/content/pkg/BUDGET-2010-TRS/pdf/BUDGET-2010-TRS.pdf.

[41] *Frank Liobondo Coast Guard Authorization Act of 2018*, Public Law 115-282, 115th Cong., 2nd sess., December 4, 2018, https://www.congress.gov/115/plaws/publ282/PLAW-115publ282.pdf.

[42] Aaron Martin, "Senate Bill Would Require Establishment of Land-Based Alterative to GPS Satellite Timing Signals," *Homeland Preparedness News*, December 19, 2017, https://homelandprepnews.com/stories/25836-senate-bill-require-establishment-land-based-alternative-gps-satellite-timing-signals/; Athanasios K. Goudosis and Sokratis K. Katsikas, "Secure AIS with Identity-Based Authentication and Encryption," *TransNav* 14, no. 2 (June 2020), 287–298, http://dx.doi.org/10.12716/1001.14.02.03; Gary C. Kessler, "Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity," *TransNav* 14, no. 2 (June 2020), 279–286, http://dx.doi.org/10.12716/1001.14.02.02; "PNT ExCom Backs eLoran as a Step to Full GPS Backup System," *Inside GNSS*, December 10, 2015, https://insidegnss.com/pnt-excom-backs-eloran-as-a-step-to-full-gps-backup-system/.

[43] Kessler and Shepard, *Maritime Cybersecurity.*

[44] Kessler and Zorri, "Cross Domain IW Threats to SOF Maritime Missions."

[45] Baorong Yan et al., "High-Accuracy Positioning Based on Pseudo-Ranges: Integrated Difference and Performance Analysis of the Loran System," *Sensors* 20, no. 16 (August 2020), 4436, https://doi.org/10.3390/s20164436; Dana Goward, "China Expanding Loran as GNSS Backup," *GPS World*, October 12, 2020, https://www.gpsworld.com/china-expanding-loran-as-gnss-backup/; Wenhe Yan et al., "An eLoran Signal Cycle Identification Method Based on Joint Time–Frequency Domain," *Remote Sensing* 14, no. 2 (January 2022), 250, https://doi.org/10.3390/rs14020250.

[46] Michael J. Biercuk and Richard Fontaine, "The Leap Into Quantum Technology: A Primer for National Security Professionals," *War on the Rocks*, November 17, 2017, https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/.

[47] Christine Bonniksen, "Global Differential GPS (GDGPS) System Future," National Aeronautics and Space Administration, Space-Based Position Navigation and Timing National Advisory Board Meeting, July 1, 2020, https://www.gps.gov/governance/advisory/meetings/2020-07/bonniksen.pdf.

[48] Dana Goward, "China Leads World With Plan for 'Comprehensive' PNT," *GPS World*, November 14, 2019, https://www.gpsworld.com/china-leads-world-with-plan-for-comprehensive-pnt; David H. Millner, Stephen Maksim, and Marissa Huhmann, "BeiDou: China's GPS Challenger Takes Its Place on the World Stage," *Joint Force Quarterly* 105 (2nd Quarter 2022), 23–31, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2999161/beidou-chinas-gps-challenger-takes-its-place-on-the-world-stage/.

[49] Garath Wimpenny et al., "Securing the Automatic Identification System (AIS): Using Public Key Cryptography to Prevent Spoofing Whilst Retaining Backwards Compatibility," *Journal of Navigation* 75, no. 2 (2022), 333–345.

[50] Kessler and Shepard, *Maritime Cybersecurity.*

Linemen contracted by U.S. Army Corps of Engineers prepare to be sling-loaded from helicopters to inspect tops of high-voltage transmission towers and anchor lines that hold them in place after roughly 80 percent of grid was affected by storms, Aguadilla Pueblo, Puerto Rico, February 16, 2018 (U.S. Army Corps of Engineers/Michael N. Meyer)

Microgrids for the 21st Century

The Case for a Defense Energy Architecture

By Steven Curtis and Peter D. Rocha

Captain Steven Curtis, USA (Ret.), is a Consultant at the Readiness Resource Group. Colonel Peter D. Rocha, USAR, is a Faculty Instructor at the U.S. Army War College.

The Department of Defense (DOD) needs a new approach to electrical grid infrastructure to maintain security and access to operational energy. Recent natural disasters and cyber attacks have exposed the vulnerability of the current system, posing threats to military operational readiness. Strategic military facilities currently acquire most of their electric power directly from the national grid, which is increasingly vulnerable to failures. The problems experienced to date could be exponentially worse if targeted by a sophisticated adversary with advanced offensive cyber capabilities, such as Russia or China. Simultaneously, the growth of renewables and increased DOD demand for carbon-free energy create challenges and opportunities for operational energy. To date, only a small fraction of work has been done to create a system for DOD energy that is robust, responsive, and reliable.

A Defense Energy Architecture (DEA) should address these issues by providing a comprehensive approach to microgrid implementation for defense installations and deployable energy capabilities. A DEA would simultaneously deliver increased infrastructure security and carbon-free energy with an advanced microgrid system based on small modular reactor (SMR) nuclear power and renewables, such as wind and solar, when they are available. A DEA should also emphasize the development of energy storage applications beyond batteries, specifically hydrogen. A fully integrated system of baseload (that is, on all the time) electricity production, renewables, and energy storage is necessary to maximize the benefits to DOD in both permanent installation and expeditionary environments. The focus of a DEA should be on efficient resources based on the requirements of each base in which the microgrids would be employed.

DOD needs to advance microgrid systems for several reasons. First, DOD has energy assurance and resilience needs that significantly exceed most civilian requirements, and it therefore requires a separate system for energy production and storage. Second, as one of the largest single energy consumers in the world, DOD has the scale to create a market demand signal strong enough to encourage private investment and drive down hardware costs. Finally, with suitable guidance, DOD could move quickly to reach net-zero carbon goals for energy production.

The defense grid system and energy production mechanisms must improve to increase resilience to natural disasters and terrorist attacks on the national grid and integrate clean energy improvements in a cogent manner. This article defines the concept of a Defense Energy Architecture that may guide the construction of microgrid systems to supply desired energy production while supporting energy independence, security, resiliency, and affordable power. We further recommend that DOD integrate emerging energy concepts, in both garrison and expeditionary environments. Advances in modern energy technologies provide many opportunities for DOD to modernize, increasing security and operational capabilities.

DOD Reliance on the National Electric Grid System and Vulnerabilities

The national grid was designed with one purpose: to deliver electric power from the source of production to end users. However, at the time of its creation, there was little thought given to things such as redundancy in natural disasters and certainly none given to potential problems that could not be imagined at the time, such as cyber attacks and electromagnetic pulse (EMP) weapons. For the security of the Nation, DOD must ensure that it has continuous access to energy, making the entire defense system more robust and able to withstand the emerging threats of 21st-century warfare.

America's electrical grid is the system that powers the garrison operations of DOD and provides a platform for the application of military power worldwide. For decades, the reliability of the grid system was such that the military was confident that when electricity was needed, it would be there. However, this basic assumption is being questioned as the national grid ages, shows vulnerabilities, and grapples with the challenges of incorporating distributed electricity-generating sources like solar and wind energy.[1] These shortcomings—coupled with the realization that the existing system is vulnerable to disruptions from incidents both natural (hurricanes and solar flares) and man-made (cyber attacks and EMPs)—call for more direct control by DOD of energy production systems.

However, rather than simply moving ahead with its current course, DOD should embrace best-in-class technologies to ensure that it is moving forward with the best solutions. Moreover, the system needs to be flexible enough to incorporate new technologies as they evolve to ensure that best-in-class remedies are delivered to address the changing nature of power generation and increasingly sophisticated potential attacks on critical infrastructure.

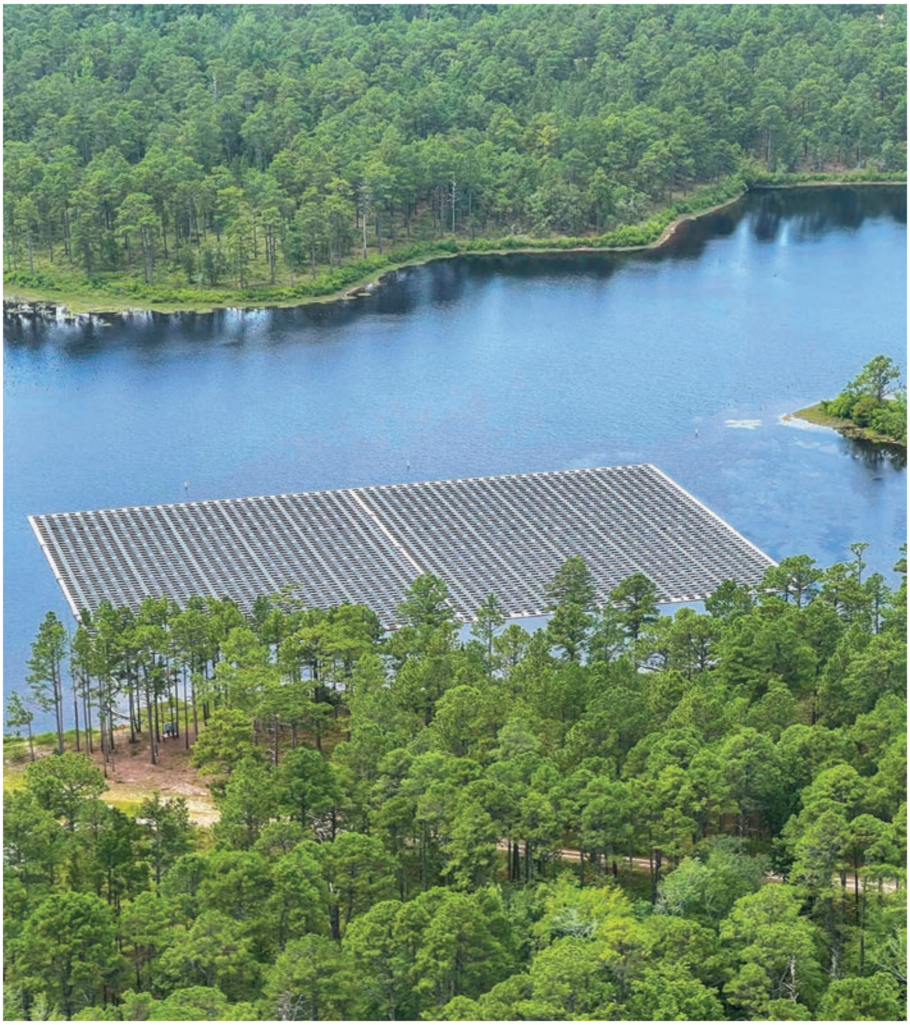
The current grid system struggles to deal with vulnerabilities that could disrupt power and harm American security, including potential attacks by foreign adversaries or terrorists. For many, Superstorm Sandy in 2012 was a wakeup call—it demonstrated a potential for widespread damage that could affect the national electrical grid, leaving 8.5 million people without power across 21 states.[2] However, to those watching closely, Sandy was not an anomalous event but rather more of a culmination of a long-term trend that has revealed how susceptible the grid is to disruption from severe weather, including wildfires and extreme temperatures.[3] The potential for disruptive events seems to be increasing.

As devastating as these natural events have been, many national security experts predict that damage from man-made attacks could be multiple times worse. The insurance company Lloyd's of London has modeled a plausible scenario in which a cyber attack on the Eastern Interconnection, which services approximately half of the United States, could leave large areas—including dozens of military installations—without power for days.[4] This is not a distant theoretical scenario: Russia has already demonstrated the ability to successfully attack electrical grid infrastructure in Ukraine, and China is believed to have similar offensive cyber capabilities.[5] Additionally, the ransomware attacks on Colonial Pipeline in 2021 demonstrated that criminal organizations and other nonstate actors also possess the tools to sow chaos in American energy infrastructure.[6] The national grid is susceptible to large-scale disruption, whether from devastating natural weather events, military attacks from near-peer competitors, or terrorists or international crime syndicates. Therefore, response readiness largely depends on a secure supply of electricity from the main grid.

We know that the military is susceptible to the same threats that menace civilian energy infrastructure. In recent years, weather events have disrupted energy service to military installations, such as Tyndall Air Force Base during Hurricane Michael in 2019 and Joint Base San Antonio–Lackland and others during the winter storms of February 2021.[7] While the effect on operations was relatively minor in these instances, it does not take much to imagine that targeted attacks on military infrastructure could be orders of magnitude more harmful and severely impact readiness. DOD recognizes this possibility and has conducted a series of exercises to better understand "the growing threat associated with natural or nefarious events . . . such as missions being separated from access to the national grid."[8] The effects from such events could have major consequences on the military's ability to respond rapidly to crises.

Defense Energy Architecture

The goal of a DEA is to ensure that the advancement of microgrids for DOD use is comprehensive and standardized. A *microgrid* can be defined as "a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously."[9] For our purposes, we believe this encompasses both energy generation and storage. Defining the concept must not only focus on near-term needs, but also keep options open for future adaptations. It is beyond the scope of this article to prescribe what a fully functional standard for a DEA would look like. However, we can outline key principles that must be addressed to answer the challenges that face the future of DOD energy systems.



Floating solar microgrid consisting of 2,700 solar panels on lake at nearby Camp Mackall provides clean energy to Fort Liberty, North Carolina, July 28, 2023 (U.S. Army/Jason Ragucci)

The following should be considered as the essential tasks for a DEA to address the emerging energy needs:

- provide carbon- and pollution-free energy and baseload power as much as possible
- provide continuous energy on demand
- provide defense against attacks and resilience in the case of natural disasters
- provide expeditionary capability.

Provide Carbon and Pollution-Free Energy

In recent years, DOD has increasingly focused on the potential threats posed by climate change. An example of this is the Army Climate Strategy, which set goals for 100 percent carbon- and pollution-free electricity for Army installations by 2030.[10] Given this policy priority, we believe a DEA should follow the same path. The current focus for the source of this energy is renewables, primarily solar and wind. However, wind and solar power suffer from the fact that they are intermittent (they supply energy only about 30 percent of the time, and wind is not predictable). This creates reliance on fossil fuel–based electrical plants to meet operational demands for energy, which not only runs counter to low carbon goals but also maintains the vulnerable linkage to the main grid.

An ideal solution to this intermittency problem is to use small modular reactors (SMRs) to integrate baseload nuclear energy as the carbon-free backup for solar and wind. In 2021, 60 percent of the electricity generated in the United States came from natural gas and coal.[11] So when renewables are not available in the desired amount, DOD and other electricity consumers plug into a system that generates over half its power from carbon-producing and -polluting resources. Instead of backing up renewables with fossil fuels, SMRs can assure that clean energy is available on demand. This shift would allow DOD to phase out fossil fuels in the energy mix over time. Each individual installation could be configured to maximize the natural resources available—for example,

Participants of Active Communications International's 9th National Conference on Microgrids toured the Otis Microgrid, DOD's first wind-powered microgrid, which provides energy resiliency for 102nd Intelligence Wing's intelligence, surveillance, and reconnaissance missions, April 16, 2019, at Joint Base Cape Cod (Massachusetts Air National Guard/Thomas Swanson)

relying more on wind for installations on the Great Plains. Once the optimal mix of renewables is designed, SMRs would be deployed to make up the balance. The units are modular and can be added to provide more energy. This would enable DOD installations to sever themselves completely from the national grid over time and achieve clean energy goals.

Provide Continuous Energy on Demand

A second aspect of a DEA is to ensure the availability of continuous operational energy. Again, the intermittent nature of renewables causes issues with instantaneous accessibility to energy. For an organization with 24/7 operational needs, this would not do. Much of the DOD focus thus far has been to look at battery storage to preserve the electricity generated by solar and wind sources.[12] However, lithium-ion batteries, which are the current state of the art, are best suited for intra-day storage, as their ability to store energy competitively is capped at around 8 hours.[13] In a normal operating environment, this is possibly adequate since it provides overnight storage and dispersion when demand for electricity is low. However, in a crisis scenario when high energy loads are present around the clock, this may lead to shortfalls. In addition, if a natural disaster took solar and wind capabilities offline, battery storage capability would be diminished rapidly after only a few hours. Therefore, a truly independent microgrid system should have autonomous power that could be provided in the case of a prolonged interruption.

While SMRs are ideal for providing continuous energy, a microgrid system should have backup power available in case the unit does need to go offline for any period. As stated, batteries have limited ability to provide anything beyond intra-day energy storage, which itself is a system vulnerability. Hydrogen has much greater capability to integrate with a microgrid system to meet energy storage needs. Hydrogen can be produced by splitting water molecules (H_20) into their component parts of H_2 and elemental oxygen. When this is done with renewable electricity, the resulting hydrogen is carbon-free or "green." Once hydrogen is formed, it can store energy indefinitely.[14] Therefore, H_2 could maximize the total amount of energy produced by renewables.[15]

Furthermore, hydrogen can be produced by nuclear power, so it is also carbon-free and can store an almost unlimited amount of energy. Infrastructure investments would be required to store the hydrogen in a safe manner, but this is currently done globally in many industries that use hydrogen. If the SMR ever went down, hydrogen could provide a long-term bridge of operational energy until the issue was resolved. Though currently less efficient for short-duration storage than batteries, the flexibility that hydrogen provides in a microgrid system makes it extremely valuable for energy assurance. In fact, coupling hydrogen with battery storage may provide the most overall benefit for the entire system.

Provide Security and Resiliency

A third requirement for a microgrid system for defense use is the ability to safeguard it from potential attacks. We have noted that one of the vulnerabilities of the current grid is susceptibility to cyber attacks. The nature of warfare is constantly evolving. A World War I–era general transported to the 21st century would barely recognize how warfare is conducted in the age of long-range missiles, precision-guided munitions, and stealth bombers. It is not difficult to believe that future warfare may become as unrecognizable to us, since the main contested spaces in the future might not be air, land, and sea but space and cyberspace.

A tipping point may have been reached already with advances in the sophistication of offensive cyber capabilities and society's increasing reliance on digital technology.[16] The national electric grid is vulnerable because of age and the threat to the Supervisory Control and Data Acquisition (SCADA) control system from cyber attacks. An additional threat comes from EMP weapons, which deliver a pulse of energy from a nuclear or electromagnetic detonation "that creates a powerful electromagnetic field capable of short-circuiting a wide range of electronic equipment," including computers and telecommunications equipment.[17] The conventional grid is exposed to EMP attacks in the form of high-voltage control cables and transformers that regulate the grid. High-voltage transformers take 2 years to build, and the United States is inadequately stocked with backup transformers. Thus, a large-scale EMP attack could bring down a large section of the grid for an extended time.[18]

Certainly, military operational readiness would suffer if military installations were still integrated in the national grid at the time of such an attack. Again, this is not a scenario found only in science fiction novels and dystopian Hollywood films. Today, China is already believed to possess super-EMP weapons and to have developed procedures to execute a first strike.[19] This rationale is arguably enough for DOD to explore alternative power delivery systems to maintain response capabilities in the event of such an assault.

Fortunately, a microgrid system based on SMR technology has significant defensive advantages to the national grid. First, by definition, a *microgrid* is a discrete system that provides power locally. An SMR acts as an "island of power," which decouples from the larger grid and from other military installations, so a successful attack on one installation would be an isolated incident and not a systemic failure. In the case of a cyber attack or EMP detonation on the larger grid infrastructure, a military microgrid would simply not be affected because it is separate from the rest of the system.

Direct cyber attacks on microgrid infrastructure are also possible, but this infrastructure is more resilient because of its independent computer control. We recommend that both buried SMRs and underground power lines are a standard part of a DEA microgrid configuration. By virtue of being below surface, they are less vulnerable to overhead EMP explosions, which is not an option for systems based on solar panels and wind turbines. Increased sophistication and sheer volume of monitoring sensors required on a large grid necessitate the automated monitoring capabilities of a SCADA system. Automation not only provides efficiency of operation but also affords efficiency of disruption if cyber security systems can be breached. A series of smaller grid systems could be better protected individually, thus vastly increasing cyber security.[20] Furthermore, the use of hydrogen as an energy storage medium provides a long-term reservoir of energy, and if the SMR were taken offline for a period, a reversible hydrogen stack could return the stored power in the form of electricity, assuming no damage to the transmission infrastructure.

Provide Expeditionary Capability

The fourth concept underpinning the DEA is the idea that any investments in energy production and storage systems should be applicable in expeditionary environments as well as at installations after the strategic systems become mature. The military uses doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) to assess organizational systems and the resources required to support those systems. DOD should avoid redundancy of DOTMLPF for separate systems for energy production and delivery in garrison and expeditionary environments. This just represents waste and opportunity cost.

Second, the challenges faced in deployed operations are equally well addressed by the microgrid systems that we advocate. In the wars in Afghanistan and Iraq, powering forward operating bases was one of the most challenging and deadly aspect of the conflicts. Diesel generators and vehicles required constant fueling, which gave the enemy ample opportunity to attack resupply convoys. The Army Environmental Policy Institute calculated that every 39 fuel-resupply missions resulted in a U.S. casualty.[21] These are lives that are lost or irreparably changed, and no price tag can be placed on them. Additionally, it has been estimated that the financial cost of delivering fuel to the end user in the operational theater exceeded $400 per gallon.[22] Given the personal and fiscal costs that result from current in-theater energy systems, the clear challenge is to develop systems that remove military operations from the "tether of logistics" as much as possible. This would not only save blood and treasure but also enhance operational flexibility of commanders since they would experience more autonomy in deploying forces.

In addition to installation energy systems, SMRs have the potential to act as the centerpiece of deployed energy systems. As DOD better understands the capabilities of mobile reactors, we expect to see the technology migrate further to the tactical level. The Navy is certainly no stranger to small nuclear reactors, as they have been employed in the fleet since the USS *Nautilus* launched in 1955. Project Pele, conducted by DOD,[23] envisions an SMR that can be used at remote operational bases.[24] Analysis has shown that SMR technology allows for production units that are small enough to be moved by a heavy truck but are large enough to produce up to 20 megawatts of energy, enough to power an Army division headquarters.[25]

As discussed, an SMR can be buried underground, making it a hard target in a deployed environment. While SMRs address the need for a forward operating base's energy, they do not directly address vehicle mobility. However, the electricity from nuclear generation can

Technical Sergeant Marquelle Willis, 23nd Civil Engineering Squadron, Moody Air Force Base, Georgia, Prime BEEF, electrical systems noncommissioned officer in charge, works to repair high-voltage power lines supplying electricity to tent city, Tyndall Air Force Base, Florida, October 28, 2018, after Hurricane Michael (U.S. Air Force/Kelly Walker)

be used to power electric and hybrid electric vehicles that the U.S. military is already experimenting with.[26] As stated, nuclear energy can be used to create hydrogen and other fuels, and higher operating temperatures of SMRs are ideal for producing hydrogen. Because hydrogen is energy-dense, it can extend the operational range of vehicles. In fact, H_2 is nearly three times as energy-dense as petroleum diesel, which means less refueling and fewer halts in missions for refueling operations.[27] These expanded operational capabilities are simply not available with batteries, which have one-hundredth the energy storage capacity of hydrogen on an equal-weight basis.[28] The nuclear-hydrogen synergy could provide all the energy needed for military operations in deployed environments and eliminate the fossil-fuel supply chain altogether.[29] We believe a Defense Energy Architecture should unequivocally embrace an SMR-hydrogen system in deployed operations to save lives and resources and increase operational range and flexibility.

DOD Role in Advancing Energy Technology

Both SMRs and green hydrogen production can be considered emerging commercial technologies. That is, there are commercial units available, but the industries have not yet scaled to optimize production costs. The general trend in technologies over time is to become smaller and cheaper as the technology evolves. However, this takes place only if demand for the product is such that the product is seen as having long-term profitability, and companies have the incentive to invest in research and development that keeps technology moving forward.

The military operates nearly 800 installations worldwide.[30] If even a fraction of these installations were to develop SMR capabilities, it would provide a clear signal to producers and investors. The first SMRs would be much less risky to financiers if they had long-term contracted customers once completed. In fact, the Special Capabilities Office (SCO) within the Office of the Secretary of Defense has already narrowed the selection for the first such SMRs to two commercial designs under Project Pele.[31] However, this project cannot be seen as a one-off event if the scale benefits for DOD are to be realized. Project Pele could drive the procurement of the first few units within years and lay out a comprehensive plan for future purchases in the out years. A similar effort to identify promising hydrogen technologies would serve to spur investment and bring down costs for long-term, flexible energy-storage options.

The current moment is favorable for this transition in energy systems. SMR designs are being developed by more than 50 startup companies with private capitalization of greater than $2 billion.[32] Instead of paying for the entire technological development cost, the

Marine Corps Colonel Thomas M. Bedell (right), commanding officer of Marine Corps Air Station Miramar, and Mick Wasco (MCAS), MCAS Miramar energy program manager, discuss microgrid and its benefits at station's Energy and Water Operations Center, on MCAS Miramar, San Diego, California, January 21, 2022 (U.S. Marine Corps/Jose S. GuerreroDeLeon)

military need only pay for the adaptation to military standards. Based on this, the SCO predicts the initial non-Navy military SMR market will be 300 units and the civilian market 1,000 units.[33] The Department of Energy (DOE)'s Office of Nuclear Energy is already collaborating with the SCO to move the project forward and coordinate national laboratory efforts. In fact, the coauthor has personally been involved in extensive meetings at Creech Air Force Base, Nevada, to discuss the possibility of "assured energy" being supplied to the base through a prototype SMR as early as 2030.

Similarly, there is much interest in advancing green hydrogen technology. DOE has launched an initiative called the Hydrogen Shot to reduce the production cost of green hydrogen by 80 percent by 2030.[34] Furthermore, the Inflation Reduction Act has announced an investment of up to $8 billion in creating regional hydrogen hubs.[35] These programs will stimulate significant private investment as well and help advance the current state of hydrogen technology. DOD can draft off these efforts to ensure that developing hydrogen technologies meet the military specifications of an advanced microgrid system. The earlier the demand signal from the military (vs. DOD hoping for the appropriate solutions to emerge organically), the more likely that customized offerings will be available. DOD can play an important role in providing a market for these emerging technologies.

Conclusion

For the military, energy is the lifeblood to maintain military capabilities. In the event of a large-scale natural disaster or infrastructure attack, the military needs to maintain its own systems to ensure readiness. For these reasons, DOD needs to keep advancing SMR-based microgrid systems with adequate long-term energy storage in the form of hydrogen. For strategic facilities, this would mean that bases control their own destiny without counting on an ever more vulnerable electric grid. With SMR microgrids, military bases can isolate their power supply from the grid when necessary. In fact, during crises, excess power could be supplied to the civilian sector as it is available.

DOD should double down on the current efforts of developing microgrids to increase the resilience of its installations, retain the ability to deploy forces globally when needed, and provide expeditionary power without exposed refueling logistics. The benefits would be multifold. In addition to decreasing vulnerability, DOD adaptation of SMR-based microgrids would allow the military to meet clean energy goals and separate itself from carbon-producing fossil fuels. Increased DOD adaptation would drive demand, resulting in greater competition and lower prices. Furthermore, it would serve as a model to civilian energy planners who could observe the positive outcomes and adapt the technology to civilian requirements.

The military has already determined that SMR microgrids have merit, as evidenced by the maturing of Project Pele. The final solution to base supply of electricity should consider long-term efficiencies to the military of the 21st century. All sources of clean energy integration should be considered on a case-by-case basis to meet the individual needs and priorities of each base mission. Success could drive a successful transition to tactical use of SMR microgrids as well.

The national electric grid is becoming vulnerable because of age and the threat of the SCADA control system being compromised through cyber attacks, EMP disruptions, intermittent power outages, or terrorist threats. Military electric power supply, both strategic and tactical, must adapt to this reality and plan for increased future use of microgrids within a generation in the name of mission assurance. Availability, affordability, and uninterrupted power are the force multiplier requirements governing the transition away from legacy systems toward independent microgrids. It is critical that a transition to a defined Defense Energy Architecture, based on these principles, be developed and implemented soon. **JFQ**

Notes

[1] Brian Warshay, "Upgrading the Grid: How to Modernize America's Electrical Infrastructure," *Foreign Affairs*, March/April 2015.

[2] Stephen Lacey, "Resiliency: How Superstorm Sandy Changed America's Grid," *Green Tech Media*, June 10, 2014, https://www.greentechmedia.com/articles/featured/resiliency-how-superstorm-sandy-changed-americas-grid.

[3] Ibid.

[4] Robert K. Knake, *A Cyberattack on the U.S. Power Grid* (New York: Council on Foreign Relations, April 2017), https://www.cfr.org/report/cyberattack-us-power-grid.

[5] Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Director of National Intelligence, January 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—-SSCI.pdf.

[6] David E. Sanger, Clifford Krauss, and Nicole Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *New York Times*, May 8, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

[7] Rose L. Thayer, "Winter Weather Causes More Than a Dozen Military Bases to Close," *Stars and Stripes*, February 16, 2021, https://www.stripes.com/theaters/us/winter-weather-causes-more-than-a-dozen-military-bases-to-close-1.662417.

[8] Rachel S. Cohen, "DOD's 'Black-Start' Exercises Explore What Happens When Utilities Go Dark," *Air & Space Forces Magazine*, October 17, 2019, https://www.airforcemag.com/dods-black-start-exercises-explore-what-happens-when-utilities-go-dark/.

[9] Allison Lantero, "How Microgrids Work," *Breaking Energy*, July 20, 2015, https://breakingenergy.com/2015/07/20/how-microgrids-work-2/.

[10] Department of the Army, Office of the Assistant Secretary of the Army for Installations, Energy, and Environment, *United States Army Climate Strategy* (Washington, DC: Headquarters Department of the Army, February 2022), https://www.army.mil/e2/downloads/rv7/about/2022_army_climate_strategy.pdf.

[11] "Electricity Explained: Electricity Generation, Capacity, and Sales in the United States," U.S. Energy Information Agency, June 30, 2023, https://www.eia.gov/energyexplained/electricity/electricity-in-the-us-generation-capacity-and-sales.php.

[12] National Renewable Energy Lab (NREL), "'Fort Renewable' Shows Benefits of Batteries and Microgrids for Military and Beyond," *NREL*, July 27, 2021, https://www.nrel.gov/news/program/2021/fort-renewable-shows-benefits-of-batteries-and-microgrids-for-military-and-beyond.html.

[13] Jonathan Spencer Jones, "The Different Types of Energy Storage and Their Opportunities," *Smart Energy International*, May 14, 2021, https://www.smart-energy.com/storage/the-different-types-of-energy-storage-and-their-opportunities/.

[14] Mark Newton, "Is Hydrogen Storage the Future of Renewable Energy?" *Reset*, June 27, 2022, https://en.reset.org/is-hydrogen-storage-the-future-of-renewable-energy/.

[15] NREL, "Answer to Energy Storage Problem Could Be Hydrogen," *NREL*, June 25, 2020, https://www.nrel.gov/news/program/2020/answer-to-energy-storage-problem-could-be-hydrogen.html.

[16] Peter Yeung, "Why Cyber Attacks Will Define 21st-Century Warfare," *Raconteur*, August 26, 2021, https://www.raconteur.net/technology/why-cyber-attacks-will-define-21st-century-warfare.

[17] Washington State Department of Health, "Electromagnetic Pulse (EMP)," Fact Sheet 320-090, September 2003, 3, https://doh.wa.gov/sites/default/files/legacy/Documents/Pubs/320-090_elecpuls_fs.pdf.

[18] James Conca, "China Has 'First-Strike' Capability to Melt U.S. Power Grid With Electromagnetic Pulse Weapon," *Forbes*, June 25, 2020.

[19] Ibid.

[20] *Terrorism and the Electric Power Delivery System* (Washington, DC: National Academies Press, 2012), https://nap.nationalacademies.org/catalog/12050/terrorism-and-the-electric-power-delivery-system.

[21] David S. Eady et al., *Sustain the Mission Project: Casualty Factors for Fuel and Water Resupply Convoys* (Arlington, VA: Army Environmental Policy Institute, September 2009), 14, https://apps.dtic.mil/sti/pdfs/ADB356341.pdf.

[22] Adam Tiffen, "Going Green on the Battlefield Saves Lives," *War on the Rocks*, May 22, 2014, https://warontherocks.com/2014/05/going-green-on-the-battlefield-saves-lives/.

[23] "Project Pele: Mobile Nuclear Reactor," Office of the Under Secretary of Defense for Research and Engineering, n.d., https://www.cto.mil/pele_eis/.

[24] Jaroslaw Gryz et al., "Mobile Nuclear-Hydrogen Synergy in NATO Operations," *Energies* 14, no. 23 (2021), 6, https://www.proquest.com/openview/21c797e164840e6b525ba8343e949115/1?pq-origsite=gscholar&cbl=2032402.

[25] Ibid., 7. See also "U.S. Army Signs onto 20 MW Solar Farm, Biggest in Military," *GreenBiz*, April 12, 2013, https://www.greenbiz.com/article/us-army-signs-20-mw-solar-farm-biggest-military.

[26] Jen Judson, "Oshkosh Unveils Hybrid Electric Joint Light Tactical Vehicle," *Defense News*, January 25, 2022, https://www.defensenews.com/land/2022/01/25/oshkosh-unveils-hybrid-electric-joint-light-tactical-vehicle/.

[27] Patrick Molloy, "Run on Less With Hydrogen Fuel Cells," *RMI*, October 2, 2019, https://rmi.org/run-on-less-with-hydrogen-fuel-cells.

[28] Gryz et al., "Mobile Nuclear-Hydrogen Synergy in NATO Operations," 9.

[29] Ibid.

[30] David Vine, "Where in the World Is the U.S. Military?" *Politico*, July/August 2015, https://www.politico.com/magazine/story/2015/06/us-military-bases-around-the-world-119321/.

[31] Aaron Mehta, "Pentagon Awards Contracts to Design Mobile Nuclear Reactor," *Defense News*, March 9, 2020, https://www.defensenews.com/smr/nuclear-arsenal/2020/03/09/pentagon-to-award-mobile-nuclear-reactor-contracts-this-week/.

[32] John Milko, Jackie Kempfer, and Todd Allen, "2019 Advanced Nuclear Map," *Third Way*, October 17, 2019, https://www.thirdway.org/graphic/2019-advanced-nuclear-map.

[33] Patrick Tucker, "U.S. Military Eyes Tiny Nuclear Reactors for Deployed Troops," *Defense One*, January 24, 2019, https://www.defenseone.com/technology/2019/01/us-military-eyes-tiny-nuclear-reactors-deployed-troops/154406/; and author teleconference meeting April 16, 2019, with the National Defense Industrial Association–Las Vegas and the Special Capabilities Office.

[34] Department of Energy, "Hydrogen Shot," Office of Energy Efficiency and Renewable Energy, 2021, https://www.energy.gov/eere/fuelcells/hydrogen-shot.

[35] Department of Energy, "Regional Clean Energy Hubs," Office of Clean Energy Demonstrations, n.d., https://www.energy.gov/oced/regional-clean-hydrogen-hubs.

Then Chairman of the Joint Chiefs of Staff General Mark A. Milley congratulates National War College graduate during National Defense University's 2023 graduation ceremony, June 8, 2023, on Fort Lesley J. McNair, Washington, DC (NDU Audio Visual)

A New Form of Accountability in JPME

The Shift to Outcomes-Based Military Education

By Kristin Mulready-Stone

The programs responsible for teaching joint professional military education (JPME) Phases I and II are in the early stages of a significant overhaul of how they demonstrate to the Joint Staff that they are fulfilling their mission of educating and developing leaders from the U.S. joint force, interagency community, and officers from allied and partner countries around the world. These institutions of higher education operate under the Officer Professional Military Education Policy (OPMEP), the latest version of which is OPMEP Foxtrot (OPMEP-F).[1] Under previous versions, JPME programs were required simply to demonstrate they were covering the content that congressional statutes require them to deliver. That process was assumed sufficient to ensure that the programs were teaching what needed to be taught and that students were learning what they needed to learn. OPMEP-F, released on May 15, 2020, introduced a wholesale change in how JPME pro-

Kristin Mulready-Stone is Professor and Director of the Writing and Teaching Excellence Center at the U.S. Naval War College, and in 2023–2024, a Visiting Professor and the Harold K. Johnson Chair of Military History at the U.S. Army War College.

grams will have to prove to the Joint Staff that they are accomplishing their objectives, specifically by demonstrating their graduates have reached the appropriate level of achievement on defined learning outcomes. Mandating that JPME programs adopt this process represents a shift to outcomes-based military education (OBME).[2]

This shift in methodology brings JPME in line with standard practice across postsecondary education in civilian academia—not only in the United States but also in higher education across much of the world—through a practice commonly known as *assessment* in outcomes-based education.[3] This article serves as a primer on this kind of assessment for JPME faculty and administrators and anyone interested in JPME. It introduces some of the terminology, explains some of the benefits, provides a brief historical overview, points out strengths in the shift to OBME so far, and identifies caveats as JPME progresses through the shift to OBME.

In civilian higher education, the terms *assessment*, *outcomes-based education*, and variations such as *outcomes assessment* are used interchangeably. The fundamental intention underlying assessment is to ensure that students are in fact learning what their professors, departments, and programs intend for them to learn. This represents a change in emphasis in JPME programs' accountability from merely proving they are covering the required content to additionally providing evidence that graduates have reached a sufficiently high level of achievement of Program Learning Outcomes (PLOs) through a process referred to as *measuring outcomes.* In other words, JPME programs now are not only required by statute to cover certain content and assign, grade, and provide feedback on papers, exams, and other projects, but they must also institute a new evidence-based process specifically designed to determine whether students are reaching a sufficiently high level of achievement on what their programs intend for them to learn, as articulated in a program's learning outcomes.

The Joint Staff coined the term *outcomes-based military education* to describe this expansion in focus from content alone (covering statutory requirements) to content and outcomes (covering the content and demonstrating students have learned what they are supposed to learn) under OPMEP-F. Central to this process is that all programs develop their own PLOs that accurately reflect their unique emphases on areas such as maritime power, airpower, land-based warfare, intelligence operations, or cyber warfare, among others. Variations among the programs are expected and valued, with the caveat that all PLOs must sufficiently align with six Joint Learning Areas identified by the Joint Staff.[4] This is necessary since all programs are delivering JPME, and there must be enough commonality among them to ensure that graduates from every school have the requisite knowledge and abilities in areas that include jointness, warfighting, strategy, and the profession of arms.[5]

There are many challenges associated with a shift to outcomes-based education, not least of which is ensuring that administrators, faculty, students, and external stakeholders not only appreciate the value of assessing outcomes but also understand the difference between grading assignments and assessing outcomes.[6] A common response from faculty hearing about assessment for the first time is, "I assess my students all the time. I grade their papers and exams, I evaluate their understanding of the readings through their class participation, and I assign grades. I'm assessing them." But grading is *not* outcomes assessment.

One vivid example of how assessment provides different information than grading presented itself at the Naval War College early in our assessment efforts. All the JPME core departments developed their Course Learning Outcomes (CLOs), which articulate what students should know and be able to do at the end of a particular *course*, as opposed to PLOs, which define what they should know and be able to do after taking all the required courses in a JPME *program.* One of the departments had carefully developed CLOs that were an accurate reflection of what the department intended students to learn. But when it came time to map existing course assignments to those CLOs—ensuring that each assignment is clearly linked to one or more of the CLOs and allows students to demonstrate sufficient achievement of those CLOs through their coursework—this department found that the research paper that students spent most of the term working on did not actually align with any of the department's declared CLOs. This meant that a student could write a very good research paper, get a high grade on it, learn a great deal about the topic, but not make progress toward achieving the CLOs, despite having devoted dozens or hundreds of hours over the course of many weeks to research and writing.

That is, the department discovered it had assigned a task that was insufficiently connected to what that department thought its students should learn. If any assignment—let alone the most time-consuming assignment in a course—does not contribute to a student achieving the outcomes of a course or a program, this is a problem that must be remedied. Simply grading the research papers had not revealed the problem. Developing outcomes and assessing students' mastery of those outcomes through the research paper, on the other hand, threw the problem into stark relief.[7]

Realizing that an assignment does not directly contribute to students' achieving the specific course or program outcomes does not necessarily mean the faculty should eliminate the assignment—instead, they should adjust so it clearly aligns with CLOs and PLOs. In the case of this course's research paper, one possible fix would be to change the guidance to students on appropriate research topics so that conducting research and writing the paper contribute to a specific course learning outcome. In this example, the assessment process made clear that although the research paper was not in line with intended learning outcomes, relatively minor adjustments would solve the problem, strengthen student learning, and improve mastery of outcomes.

This kind of revelation about the utility of an assignment can easily be missed in the absence of a carefully designed assessment process. Nevertheless, until the process is developed, operationalized, and generating useful data and insights, faculty resistance in both civilian and military schools to a new outcomes-based assessment requirement is common, expected, and often pronounced. This is unsurprising since a new mandate to conduct assessment affects all teaching faculty, occupying time they could otherwise devote to teaching, research, writing, and publishing, and it can feel like just the latest arbitrary requirement that noneducators are inflicting on educators. Many faculty believe outcomes-based assessment will simply go away if they ignore it long enough. JPME programs should be prepared for similar faculty responses based on a decades-long pattern of such a response in civilian higher education. Tammie Cumming, L. Jay Deiner, and Bonne August emphasize the importance of respecting people's time when shifting to outcomes-based education, noting:

> *Colleges and universities are busy places where everyone is balancing multiple competing priorities; time is the greatest commodity. Faculty, staff, and administrators will quickly come to resent anything that requires a large investment of time for little payoff. Therefore, it is critical to examine the assessment process to make sure that busywork and time burdens are minimized.*[8]

The requirement to assess learning outcomes is new in JPME, and many faculty are unaware of how standard these outcomes-assessment requirements are in higher education. The fact that outcomes assessment is so well established in civilian academia means that there are many lessons that JPME programs could and should learn from their civilian counterparts, such as avoiding making outcomes assessment more time-consuming than necessary and other pitfalls.

Even many faculty involved in outcomes assessment at civilian institutions, however, are unaware of its long history, and it is worth having some familiarity with it. What is recognizable today is that outcomes assessment in higher education developed over the course of several decades and has endured and grown for 30 years. In "History and Conceptual Basis of Assessment in Higher Education," Peter Ewell and Tammie Cumming provide a detailed overview of strategies designed to remedy an array of problems in postsecondary education from the 1960s onward that were the unintentional starting point of outcomes assessment. The issues included "academic and social integration" on campuses to prevent student attrition, mandatory program evaluation that came with large-scale Federal programs in the 1960s and 1970s, and "the wider movement toward 'scientific' management that quickly found applications in higher education in the form of strategic planning, program review, and budgeting," among others.[9] Ewell and Cumming emphasize that the methods developed in an effort to solve such problems coalesced over the course of a few decades into a methodology for outcomes assessment.

Three different approaches to assessment appeared in the 1970s and 1980s, all of which endure in different contexts, but they are not all part of assessment in postsecondary education today. The first focuses on an individual student's learning and is rooted in "development over time and continuous feedback on individual performance." The second is now inextricably linked to accountability in K-12 education and was designed not "to examine individual learning, but rather to benchmark school and district performance." The third "defined *assessment* as a special kind of program evaluation, whose purpose was to gather evidence to improve curricula and pedagogy. . . . This tradition focused on determining aggregate not individual performance."[10] By the mid-1980s there was enough (though by no means universal) discussion in higher education circles of improving student learning through outcomes assessment that the First National Conference on Assessment in Higher Education, cosponsored by the National Institute of Education (NIE) and the American Association for Higher Education, was held in Columbia, South Carolina, in fall 1985. Ewell and Cumming make clear that "the proximate stimulus for the conference was a report called *Involvement in Learning*," published by NIE in 1984:

> *Three main recommendations formed its centerpiece, strongly informed by research in the student learning tradition. In brief, they were that higher levels of student achievement could be promoted by establishing high expectations for students, by involving students in active learning environments, and by providing them with prompt and useful feedback. But the report also observed that colleges and universities as institutions could "learn" from feedback on their own performances and that appropriate research tools were now available for them to do so.*[11]

The feedback that colleges and universities could glean from assessment would allow them to adjust not only content but also teaching methodologies when the assessment data they gathered showed that in an aggregate sense, students were not learning everything their degree programs intended them to learn. This is the piece that evolved into the approach that is now nearly universal in civilian higher education and that informs the Joint Staff's guidance for JPME institutions to follow as the schools shift to OBME.

Determining the gaps in student learning can allow departments and programs to home in on a content area that needs greater emphasis or a pedagogical method that might need adjustment.[12] The shift to focusing on assessment processes and measuring outcomes took higher education away from an earlier input-based standard—a different set of metrics that did almost nothing to demonstrate that students had learned what they were supposed to learn. Before the 1980s, as Kenton Fulcher and Caroline Prendergast make clear in their book on improving student learning, "institutional quality was evaluated almost entirely on inputs (e.g., number of faculty holding doctoral degrees, test scores of incoming students) and outputs (e.g., graduation rates, employment rates of graduates)."[13] Faculty credentials are important. Students graduating and finding employment are also important. But these inputs and outputs do not provide any evidence that students have learned what is necessary for them to do "what is essential for all students to be able to do

Naval War College holds commencement ceremony for College of Naval Command and Staff and College of Naval Warfare 2023 graduating classes, June 16, 2023, on board Naval Station Newport, Newport, Rhode Island (U.S. Navy/Kristopher Burris)

successfully at the end of their learning experiences," which is the central requirement of outcomes-based education, the approach to education the Joint Staff has now embraced.[14]

That said, there needs to be more to the outcomes-assessment process than simply developing assessment mechanisms and compiling data in line with the practice of outcomes-based education. Compiling the data on mastery of outcomes does not in any way guarantee better results in teaching and learning than the inputs-outputs approach. The essential—and frequently overlooked—final step in the process is to evaluate the data and adjust curricula and teaching methodologies to improve student learning, which would lead to higher levels of student mastery of the outcomes. There are plenty of examples of colleges and universities devoting countless hours of faculty time to assessing outcomes and compiling data, then failing to *close the loop*. That is, they fail to come up with effective processes to evaluate the data and to apply the lessons the data yield back into the curriculum in ways that result in better student achievement of outcomes.[15] As Fulcher and Prendergast succinctly state, "Assessment should not be treated as an end unto itself. Instead, the rightful emphasis should be placed on improving student learning."[16] Their research followed an important 2018 National Institute for Learning Outcomes Assessment (NILOA) report that concluded:

> *While use of assessment results is increasing, documenting improvements in student learning and the quality of teaching falls short of what the enterprise needs.* [In a 2017 NILOA survey], *provosts provided numerous examples of expansive changes at their institutions drawing on assessment data, but too few had examples of whether the changes had the intended effects.*[17]

Closing the loop by improving student learning is the most crucial step; if this step is overlooked or carried out half-heartedly or ineffectively, all the faculty time devoted to coming up with learning outcomes, measuring those outcomes through well-developed assessment mechanisms, and compiling the data would ultimately amount to nothing more than wasted time. Adjustments need to be made, and then programs must reassess the outcomes to determine whether student achievement on outcomes improved.

Wanda Baker of Council Oak Assessment pointed out at the fall 2021 annual Assessment Institute at Indiana University–Purdue University Indianapolis that colleges and universities have been measuring outcomes and compiling data and filling countless binders with data that then sit on shelves in someone's office, ultimately accomplishing nothing. But when the data sits on a shelf in a binder and does nothing to help students learn what they should be learning, it boils down simply to a box-checking exercise to keep accreditors off an institution's back rather than an admittedly time-consuming but worthwhile enterprise to improve teaching and learning.[18] Wasting faculty time by failing to close the loop is an endstate JPME institutions must avoid.

Encouraging Signs

Guidance so far from the Joint Staff J7 on how programs should make the transition to OBME has been clear and overall positive.[19] Those who drafted OPMEP-F did a thorough job of educating themselves on outcomes assessment, and the document does

General Darren W. McDew, then commander of U.S. Transportation Command, Scott Air Force Base, Illinois, presents lecture to Marine Corps War College students at Dunlap Hall, Marine Corps University, Quantico, Virginia, March 6, 2018 (U.S. Marine Corps/Kathy Reesey)

capture its true intent and purpose, aligning with the assessment scholarship. OPMEP-F also comes with a procedures manual, published on April 1, 2022, which gives detailed instructions on how to develop learning outcomes, provides guidance to ensure the outcomes align with institutions' and programs' mission statements, and defines seven milestones each program has to pass to achieve full certification from the Joint Staff J7.[20] Programs have 6 years from the publication of the OPMEP-F manual to complete this process.[21] This is ample time, particularly given that a near-final draft of the manual was sent to all JPME programs in summer 2021. Even though the manual had not yet been signed, some JPME institutions were able to start the milestones process in summer and fall 2021 based on its guidance. Even institutions that were not yet ready to begin the process were able to make progress toward the early milestones with the draft manual in hand, meaning all schools and programs will have more than 6 years to gain OBME certification.

A central component of the milestones process is the requirement to report PLO assessment data for 4 full years before a program can achieve full certification under OBME. This requirement is appropriate for two reasons. First, that amount of time will allow programs to test their assessment mechanisms and make any necessary adjustments to ensure they are effective in assessing PLOs and generate the necessary data on student learning and achievement. Second, and just as important, the literature on closing the loop makes clear that improved learning cannot happen in 1 year, rarely happens in 2 years, but takes 3 or more years before efforts to improve curricula or methodologies will show up in the data.[22] With 4 years of data, JPME programs that develop sound processes for closing the loop will be able to report on the early signs of how effective their OBME practices are and what they intend to do to make them even more robust. This will be true for 10-week and 10-month resident programs and for distance programs that take longer to complete.

Another important part of the OBME certification process is that the OPMEP-F manual specifies that JPME programs will report on their 4 years of assessment data in *biennial reports*, not annual reports, reporting 2 years of data at a time.[23] This provides time to assess PLOs and reflect on the significance of the data, so programs can develop a clear plan on how to close the loop to improve student learning. Indeed, the definition of *assessment* in OPMEP-F is, "The systematic collection, review, and use of information to improve student learning."[24]

The review and use of the information collected through assessment requires deliberation and reflection time. By year 4, there should be opportunity for programs to have adjusted to close the loop and for those efforts to show up in the data. This process will by no means be complete at the time of the second biennial report, but for programs that take this challenge seriously, the 4 years of data will provide sufficient evidence for the OBME review teams, the Military Education Coordination Council Working Group (MECC WG), and the J7 to determine whether each program's assessment process is in line with guidance in OPMEP-F and the manual and sufficiently well developed to warrant full certification under OBME.

But the need to close the loop on student learning, although present in OPMEP-F, does not currently receive enough emphasis. As civilian institutions have learned—often painfully—collecting and reporting outcomes data *does not*, in and of itself, bring improved student performance on outcomes. Improving student learning takes time and effort, and sometimes initial efforts to improve wind up failing.

Caveats

It will be crucial, however, for the members of OBME teams, the MECC WG, and the J7 to recognize that a rigid expectation of rapid improvement will undermine the whole process. This could be challenging in an educational system whose faculty and administration report to flag and general officers, many of whom will be in place for only 2 or 3 years, and some of whom might demand faster results. Likewise, those with final authority for JPME in the J7 and the Joint Chiefs of Staff are also flag and general officers who might have similar inclinations.

In the context of the return of strategic competition with China and Russia, there is a sense of urgency for JPME to ensure that it is preparing future leaders for the new environment right now, and that expectation is understandable. Curricular changes in JPME programs to incorporate more China-focused content are well underway, and there are also discussions about increasing Russia content. Although curricular changes cannot happen overnight and a mandate from above to inject certain content into the curriculum cannot be implemented when the curriculum is already finalized for an academic term, reasonable changes can happen from one year to the next.

But the data on which learning outcomes show insufficient student achievement must be permitted to speak for themselves, as faculty and programs implement adjustments to program delivery over the course of 3 to 4 years: initial assessment to determine the baseline, followed by intervention intended to bring improvement, followed by reassessment to determine whether improvement occurred. This involves a continuing cycle of gathering and analyzing data, attempting to close the loop, then repeating the process to guide the next effort to close the loop. This process must be intentional, deliberate, and data-driven. Demands that the loop be closed without enough time to develop the right solution for a particular pedagogical shortcoming or curricular omission, or that a reassessment happen before the remedy has had time to affect outcome achievement, will sabotage the entire assessment process.

The importance of the "feedback-improvement loop" is spelled out clearly in the OPMEP-F manual.[25] It is important, however, to emphasize that the focus needs to be on longer term rather than shorter term improvement. The OPMEP-F manual states formative assessments that reveal shortcomings during a student's time in a JPME program allow "a corrective feedback loop to ensure learners achieve mastery of the materials before graduating" and that faculty "use formative assessments to identify when their students are straying from the path of PLO mastery and intervene appropriately."[26] Even though formative assessments will point out some individual problems and allow some course correction, it is not reasonable to assume that *all* students will achieve mastery on *all* PLOs every year. (This is true at all levels of education, civilian and military.) But assessing outcomes at the aggregate level will provide insight into shortcomings

#BringBackOurGirls
Time is Running Out
Countering Boko Haram in Nigeria:
Gender, Politics and Violence
NATIONAL DEFENSE UNIVERSITY

National Defense University's College of International Security Affairs hosts its annual Thesis Symposium, where students from Class of 2019 present their theses to faculty and fellow students, June 5, 2019 (NDU/Katie Persons Lewis)

Servicemember asks question of Major General James E. Taylor, Inter-American Defense College director, at event held for Army War College students at National Defense University, Washington, DC, February 3, 2023 (U.S. Air Force/Mozer O. Da Cunha)

in the courses or program, rather than at the individual level. And by necessity, the greater focus in improving student learning will have to be on making improvements year by year, not day by day, because, as stated, it takes time to interpret assessment data and determine what teaching methodology and curricular adjustments will yield a higher percentage of students mastering learning outcomes.

In addition to resisting the temptation to force a faster feedback-improvement loop, there are other caveats for JPME programs and senior leaders to keep in mind if OBME is to succeed. First and foremost, as stated in OPMEP-F, the process must remain faculty-driven, from developing and adjusting the PLOs to implementing and adjusting assessment mechanisms to creating assessment rubrics. JPME faculty have the clearest understanding of their curricula. For institutions to develop appropriate PLOs, assessment mechanisms, and rubrics, the faculty must not simply be involved, but they must also have the lead and work across departments to develop and refine PLOs, assessment mechanisms, and the feedback-improvement loop. Typically, in both civilian academia and JPME, PLOs for programs that include courses from more than one department are developed through coordination, often in the form of an assessment committee that has representatives from all departments. Although the products the faculty develop must be subject to the review and approval of the administration, faculty experts must be the primary developers.

There are potential pitfalls, however, to placing faculty at the center of developing assessment processes. Some may have prior assessment experience from civilian or military institutions of higher education where the approach too often has been all about compliance—the ineffective practice of compiling assessment data on outcomes because an accreditor requires it but failing to apply that data to learning improvement. Promoting that mindset in the OBME context would be a mistake. Others may believe they do not need any further professional development to improve student learning. As Fulcher and Prendergast point out:

> [Many faculty] *have a good sense of students' needs. It is unsurprising, then, for them to expect they could invent effective interventions without reviewing additional literature. Certainly, we would anticipate that some interventions developed this way would lead to successful learning improvement projects. However, researchers around the world have spent untold hours cumulatively studying interventions related to a massive array of educational topics and skills. Why not take the time to learn from this work from the beginning of the intervention development stage? Why not combine lessons from the literature with lessons from instructors' experiences and wisdom?*[27]

Why not, indeed? There are two great starting points for faculty development in assessing and improving student learning. One is the annual Assessment Institute in Indianapolis, which has multiple tracks that focus on different aspects and different stages of the assessment process. Each year the Assessment Institute has sessions appropriate for assessment newcomers, seasoned experts, and everyone in between.[28] The second consists of professional organizations that specialize in teaching, learning, and assessment. These organizations have websites with a wide array of assessment and learning improvement materials, and they frequently collaborate to produce such resources. The Association for the Assessment of Learning in

Higher Education has worked with the American Association of Colleges and Universities, NILOA, the American Institutes for Research (now part of Cambium Learning Group), and the POD Network (North America's largest educational development community) to assist institutions of higher education in developing and refining their faculty development and assessment processes.[29]

JPME institutions should not try to reinvent the wheel but can draw on extensive assessment expertise that has developed in civilian higher education in the past few decades to develop and refine OBME assessment mechanisms. Reading the literature is an important first step, but there are experts who can be brought to JPME campuses to do small- and large-group faculty development sessions tailored to whatever stage a particular program has reached in assessment. Some of these experts will also be experts on Officer Professional Development (OPD), but given how long outcomes-based education and assessment has been going on in civilian academia, JPME institutions can also benefit from assessment experts who do not have OPD experience. JPME programs that ignore the deep well of experience and expertise that genuine assessment experts at civilian institutions possess would sacrifice important opportunities to learn from them.

Moreover, JPME institutions must be willing to invest in necessary technology and human capital. In a 2021 Assessment Institute session, Glenn Phillips, then of Howard University, made clear that when an institution needs additional resources for implementing effective assessment mechanisms, the administration sometimes offers to hire a person or two, when the actual requirement is a technological tool to allow existing personnel to manage, process, and interpret vast quantities of data.[30] Conversely, leadership might offer a tool when additional hires are necessary. These are not always easy waters to navigate, but faculty, staff, and administrators involved in assessment must be prepared to make a convincing case on value versus cost for the resources they need.

Finally, informal collaboration among JPME programs is already happening and should become more common. Although the Naval War College's institutional accrediting agency did not require outcomes assessment until recently, most other JPME programs' accreditors did. This means that most JPME institutions have been doing some form of outcomes assessment for several years and already had PLOs and data collection processes in place. Although the Naval War College had to start from the beginning, other JPME colleges and programs have had to make substantial changes to bring their practices in line with OBME as spelled out in OPMEP-F. Several of us involved in bringing our programs in line with OBME regularly have conversations with colleagues at other institutions on what their assessment mechanisms are, how many people they have who work on assessment, what kinds of technological tools they use to facilitate the process, and other matters. One peer institution generously allowed us to observe part of its end-of-year PLO assessment process when the COVID-19 pandemic forced it to shift online, which made it easy for us to observe. This kind of cooperation across colleges and programs, combined with a concerted effort to familiarize ourselves with the literature and best practices, will bring better results for us all.

As JPME I and II programs continue to develop and refine their assessment processes, they must do their best to incorporate the lessons learned at other institutions that are further along in the process and be open to bringing in outside experts from civilian academia to make this possible. The improvement and innovation track of the Assessment Institute—which focuses on applying assessment data to improve student learning—is still new, dating to only 2018. As a result, the scholarship on implementing the feedback-improvement loop remains limited. It would behoove JPME programs not only to embrace this part of OBME earlier rather than later for the benefit of their students and programs but also to avoid wasting time and getting negative reviews from OBME teams. This means reviewing the existing literature and being prepared to innovate with methods rooted in what has worked so far. Fulcher and Prendergast bluntly state, "Given the paucity of learning improvement examples, it is safe to say that the traditional assessment model has not successfully guided [assessment] practitioners to the promised land of learning improvement."[31] Progress in this area stalled because of the pandemic but is back on track now. To do right by our students, JPME faculty, staff, and administrators will have to embrace established best practices, keep up with the developing literature on learning improvement, and innovate new methods and practices to do our part to ensure the joint force is fully prepared for strategic competition and the next war. **JFQ**

Notes

[1] The 23 programs are listed in the official document, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 1800.01F, *Officer Professional Military Education Policy* [OPMEP-F] (Washington, DC: The Joint Staff, May 15, 2020), appendix B to enclosure A, A-B-1–A-B-11, https://www.jcs.mil/Portals/36/Documents/Doctrine/education/cjcsi_1800_01f.pdf.

[2] The initialism *OBME* appears 20 times in OPMEP-F and 229 times in its accompanying procedures manual. See Chairman of the Joint Chiefs of Staff Manual (CJCSM) 1810.01, *Outcomes-Based Military Education Procedures for Officer Professional Military Education* (Washington, DC: The Joint Staff, April 1, 2022), https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%20 1810.01.pdf.

[3] From January 2010 through October 2013, the Organisation for Economic Co-operation and Development (OECD) conducted a feasibility study and published three volumes of results from its Assessment of Higher Education Learning Outcomes (AHELO) project "across diverse national, cultural, linguistic, and institutional contexts," which demonstrates how widespread assessment in higher education has become. See *AHELO Feasibility Study Report*, vol. 1, *Design and Implementation: Executive Summary* (Paris: OECD, 2013), 2, https://www.oecd.org/education/skills-beyond-school/AHELO%20FS%20Report%20 Volume%201%20Executive%20Summary.pdf. For links to all three volumes, see "Testing Student and University Performance Globally:

OECD's AHELO," OECD, June 2014, https://tinyurl.com/mvcavk7v. In addition, the United Nations Educational, Scientific, and Cultural Organization (UNESCO) advocates for outcomes assessment in education globally and includes links to publications on assessment in the Asia-Pacific, Latin America, and sub-Saharan Africa regions on its website. See "Resources on Learning Assessment," UNESCO, May 11, 2023, https://www.unesco.org/en/learning-assessments/resources. U.S. publications on assessment often refer to the existence of assessment across continents and some of the differences that exist from one country to another. See, for example, Clifford Adelman, *To Imagine a Verb: The Language and Syntax of Learning Outcomes Statements*, Occasional Paper No. 24 (Urbana, IL: University of Illinois and Indiana University, National Institute for Learning Outcomes Assessment [NILOA], February 2015), 4, 6; Daniel J. McInerney, "Historical Study in the U.S.: Assessing the Impact of Tuning Within a Professional Disciplinary Society," *Tuning Journal for Higher Education* 6, no. 1 (November 2018), 23–24.

[4] The emphasis on joint professional military education (JPME) programs maintaining their uniqueness is explicit in CJCSI 1800.01F, 3.

[5] Six Joint Learning Areas are identified in OPMEP-F: strategic thinking and communication; the profession of arms; the continuum of competition, conflict, and war; the security environment; strategy and joint planning; and globally integrated operations. For full details on what these areas should entail, see CJCSI 1800.01F, A-A-1–A-A-2.

[6] On the importance of "communicating effectively about student learning," see Natasha A. Jankowski et al., *Assessment That Matters: Trending Toward Practices That Document Authentic Student Learning* (Urbana: University of Illinois and Indiana University, NILOA, January 2018), 25–26.

[7] The instructional design community of practice frequently refers to this process as the ADDIE Model, which stands for *analyze*, *design*, *develop*, *implement*, and *evaluate*. The model assists instructors in putting together courses that meet the needs of students and programs and includes methods to determine not only whether a course has accomplished its goals but also how to make improvements the next time the course is taught. For more on the ADDIE Model, see "ADDIE Model," University of Washington–Bothell, 2023, https://www.uwb.edu/it/addie; Amanda Kathryn Nichols Hess and Katie Greer, "Designing for Engagement: Using the ADDIE Model to Integrate High-Impact Practices Into an Online Information Literacy Course," *Communications in Information Literacy* 10, no. 2 (2016), 264–282.

[8] Tammie Cumming, L. Jay Deiner, and Bonne August, "Case Study: The New York City College of Technology Approach to General Education Assessment," in *Enhancing Assessment in Higher Education: Putting Psychometrics to Work*, ed. Tammie Cumming and M. David Miller (Sterling, VA: Stylus Publishing, 2017), 171.

[9] Peter T. Ewell and Tammie Cumming, "History and Conceptual Basis of Assessment in Higher Education," in *Enhancing Assessment in Higher Education*, 4–5. The NILOA website provides free access to many assessment articles and materials, including an excerpted version of Ewell and Cumming's "A Historical Overview of Assessment: 1980s–2000s," in *Enhancing Assessment in Higher Education*, https://www.learningoutcomesassessment.org/wp-content/uploads/2019/08/Assessment-Briefs-History.pdf.

[10] Ewell and Cumming, "History and Conceptual Basis of Assessment in Higher Education," 8. Keston H. Fulcher and Caroline O. Prendergast provide good clarifying examples of the first (continuous improvement of individual students' performance) and third (focusing on the aggregate data of all students' learning to achieve "learning improvement at scale over the course of multiple student cohorts") approaches in their book *Improving Student Learning at Scale: A How-To Guide for Higher Education* (Sterling, VA: Stylus Publishing, 2021), 8–9.

[11] Ewell and Cumming, "History and Conceptual Basis of Assessment in Higher Education," 7. Emphasis added.

[12] Because all students in JPME programs are adults, technically the term here should be *andragogy* instead of *pedagogy*. But it is common practice simply to use the word pedagogy when referring to teaching students of all ages, not just children.

[13] Fulcher and Prendergast, *Improving Student Learning at Scale*, 10. For a helpful explanation of the difference between outputs and outcomes, see Ewell and Cumming, "History and Conceptual Basis of Assessment in Higher Education," 15–16.

[14] For the full definition of *outcomes-based education* included in OPMEP-F, see CJCSI 1800.01F, GL-6.

[15] Fulcher and Prendergast, *Improving Student Learning at Scale*, 11–13.

[16] Ibid., 140. Fulcher and Prendergast draw extensively on a paper by Thomas Angelo that is more than two decades old and was on the leading edge of emphasizing the importance of closing the loop on assessment to ensure that the improvement of student learning would be the fundamental purpose of assessment. See Thomas A. Angelo, "Doing Assessment as if Learning Matters Most," *AAHE Bulletin* 51, no. 9 (May 1999), 3–6, https://www.aahea.org/articles/angelomay99.htm.

[17] Jankowski et al., *Assessment That Matters*, 26.

[18] Wanda K. Baker, "Assessment 101—Part 1 of 2 (Learning Outcomes)," Session 01A, 2021 Assessment Institute in Indianapolis (virtual), hosted by Indiana University–Purdue University Indianapolis (IUPUI), October 24, 2021. On the slow pace of change from institutions' motivations to conduct assessment being entirely to comply with accreditors' demands to a balance between compliance and improving learning, see Jankowski et al., *Assessment That Matters*, 3, 6, 8–9, 14, 16, 20, 29.

[19] J7 is the directorate for Joint Force Development and "is responsible for the six functions of joint force development: Doctrine, Education, Concept Development and Experimentation, Training, Exercises, and Lessons Learned." See "Lt. Gen. Dagvin R.M. Anderson," The Joint Staff, August 2022, https://www.jcs.mil/Leadership/Article-View/Article/2308664/lt-gen-dagvin-rm-anderson/. For additional information, see "J7 Joint Force Development," The Joint Staff, n.d., https://www.jcs.mil/Directorates/J7-Joint-Force-Development/.

[20] CJCSM 1810.01.

[21] Ibid., 1.

[22] See Keston H. Fulcher and Caroline O. Prendergast, "Six Questions to Guide Your Learning Improvement Process," Panel 14L, 2021 Assessment Institute in Indianapolis (virtual), IUPUI, October 26, 2021.

[23] CJCSM 1810.01, enclosure B, B-A-2. Programs will still report on "compliance with legislative and OPMEP requirements for high-quality delivery of Joint education." See also CJCSM 1810.01, F-A-1. The annual reports are separate from the biennial reports on assessment data.

[24] CJCSI 1800.01F, glossary, Part II—Definitions, GL-3.

[25] See CJCSM 1810.01, A-1–A-3, D-1, E-A-4.

[26] Ibid., A-1.

[27] Fulcher and Prendergast, *Improving Student Learning at Scale*, 104.

[28] To see the full programs for recent and upcoming Assessment Institutes, see the "Assessment Institute Website," https://assessmentinstitute.iupui.edu.

[29] Stephen P. Hundley, Susan Kahn, and Jeffery Barbee, "Meta-Trends in Assessment: Perspectives, Analyses, and Future Directions," in *Trends in Assessment: Ideas, Opportunities, and Issues for Higher Education*, ed. Stephen P. Hundley and Susan Kahn (Sterling, VA: Stylus Publishing, 2019), 195.

[30] See Glenn Phillips, "Picking the Provost's Pocket: Navigating Politics and Finance to Secure New Assessment Technologies," Panel 14S, IUPUI 2021 Assessment Institute in Indianapolis (virtual), IUPUI, October 26, 2021.

[31] Keston H. Fulcher and Caroline O. Prendergast, "Lots of Assessment, Little Improvement? How to Fix the Broken System," in Hundley and Kahn, *Trends in Assessment*, 160.

Players participate in Defend Forward: 2019 Critical Infrastructure War Game at U.S. Naval War College, July 25, 2019, Newport, Rhode Island (U.S. Navy/Tyler D. John)

Accelerating Cyber Leader Development

A Call to Action for Service War Colleges

By Alfredo Rodriguez III

Cyber leaders find their organizations under constant cyber attack from millions of daily intrusions disrupting everything from our electoral system to our social media feeds. The 2007 cyber attacks on Estonia, the set of cyber attacks on Iran's nuclear enrichment facility at Natanz, and the 2014 Sony Pictures data hack are a few headlines at the tip of the iceberg. Today, cyberspace provides both technological opportunity and vulnerability. Electronic banking, utilities, health care—everything seems increasingly dependent on a network of digital devices that store, process, and analyze data. The frightening reality is that the Nation is adrift in a dangerous cyberspace domain, a warfighting domain that stores, processes, and analyzes data under the uncertain eye of ill-prepared senior cyber leaders. This article is

Alfredo Rodriguez III is the Enterprise Cyber Workforce Program Manager at Headquarters, U.S. Marine Corps, Deputy Commandant for Information, Workforce Division.

Marines and civilians with Marine Corps Cyberspace Warfare Group and Marine Corps Cyberspace Operations Battalion compete in Cyber Flag 23-2, at undisclosed location, August 7, 2023 (U.S. Marine Corps/Brian Stippey)

squarely focused on a recommendation to deliberately develop senior cyber leaders within the Department of Defense (DOD) to win in this dangerous battlespace.

Despite robust defensive capabilities in this domain, attacks on the United States persist. The attackers operate on the digital battlefield without the worry of legal ramifications. In an era of strategic competition, Chinese operators push to steal intellectual property and continue to inch closer to economic and military parity with the United States. Russian operators and their proxies overtly damage public trust in the integrity of the U.S. election process and democratic institutions overall.[1] U.S. infrastructure is relentlessly probed, and criminals leverage global networks to steal assets from individuals and companies alike. This environment has the potential to mute the military instrument of power in its traditional sense. Those who understand how cyberspace shapes the world will adapt methodologies, doctrine, and practices to ensure their militaries can meet the challenges. The opening letter from Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI) in the U.S. Cyberspace Solarium Commission highlighted what is at stake: "The status quo is inviting attacks on America every second of every day. The status quo is a slow surrender of American power and responsibility. We all want that to stop."[2]

Current Posture

The 2019 National Defense Authorization Act (NDAA) charted the first U.S. Cyberspace Solarium Commission to address cyberspace challenges. This commission was an initial step at the national level to define the strategic approach to defend the United States against cyber attacks of significant consequence.[3] The Solarium report discusses the implementation of national policies to recruit, develop, and retain cyber talent and deepen the range of candidates for government service. Similarly, the DOD Cyber Strategy states:

> *The Department will adapt its institutional culture so that individuals at every level are*

knowledgeable about the cyberspace domain and can incorporate that knowledge into their day-to-day activities. Leaders and their staffs need to be "cyber fluent" so they can understand the cybersecurity implications of their decisions and are poised to identify opportunities to leverage the cyberspace domain to gain strategic, operational, and tactical advantages.[4]

Operations in cyberspace must be treated like operations in the other domains; that is, the Services must commit to the unique career fields for cyberspace officers. These officers will lead or advise on how cyberspace could help influence joint operations. There is a focus on providing highly trained, technically skilled personnel at the enlisted and warrant officer ranks, and the Services can do the same for cyberspace officer career development. Like the other domains, cyberspace requires joint officers who are developed across their careers to prepare them to lead at senior levels in command and staff assignments.[5] Current DOD cyber workforce publications seek to standardize the cyber workforce and establish the foundation on which operational forces will build. These publications are the authoritative DOD reference for coding cyber positions. They are also the foundation for enterprise qualifications for those who operate, support, and lead in the cyber domain. Services will now be accountable for the development and qualification of the employees covered by this DOD Cyber Workforce Framework (DCWF). Specifically, the publications codify the cyber work role for leaders and mandate their development.

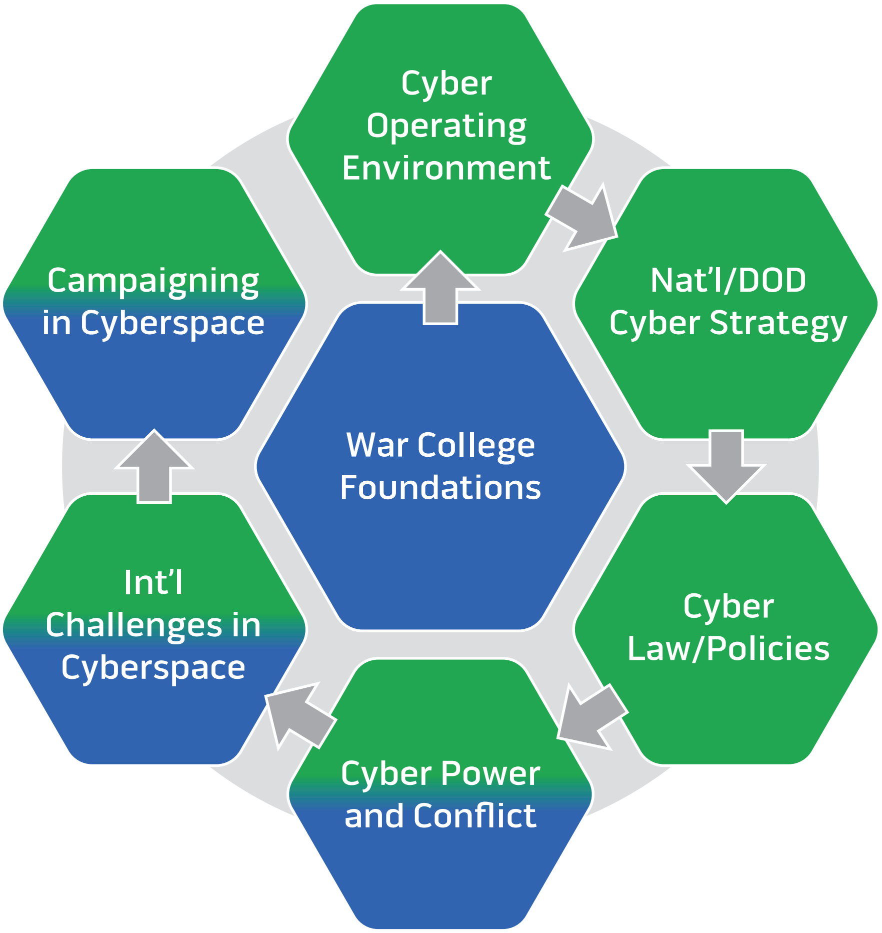
In pursuit of implementing the DCWF, how can DOD leverage the professional military education (PME) infrastructure to develop cyberspace senior military and civilian leaders? How do we prepare senior cyber leaders who will employ or advise on cyberspace and information-related capabilities in support of adaptive joint operations, strategy development, and other national security activities? These gaps prompted DOD to charter a RAND Corporation study to examine its educational institutional approach to cyberspace at the Joint PME Phase II and graduate levels.[6] The study, published just after my research into this article was concluded, recommended the same expansion this article argues for.

Service war colleges should implement a dedicated cyberspace strategic studies track aligned with the DOD Cyber Workforce Framework to develop cyberspace leaders. This pathfinder effort would shape joint PME and the future developmental ecosystem for cyberspace leaders. There must be alignment among our national and DOD strategies, joint PME guidance, and DOD cyberspace workforce directives to build such a program. This article introduces national perspectives on cyberspace, describes current DOD cyberspace workforce directives, and then details how the current joint PME apparatus is well suited to educate future cyber leaders. It concludes with a recommendation on how the Service war colleges can meet DOD requirements by instituting a cyberspace strategic studies track to help DOD succeed in the highly contested cyberspace warfighting domain.

The Cyberspace Leadership Challenge

National and DOD Perspectives. Global digital connectivity has brought us tremendous economic growth, technological dominance, and improved quality of life. The U.S. Cyberspace Solarium Commission report describes the vulnerabilities that come from people's increasing connections and the data they exchange. It notes that the cyber landscape requires a level of data security,

Figure. Cyberspace Strategic Studies Course Essentials Proposal



Note: Blue represents common course content. Green represents specialized course content. Created by author.

resilience, and trustworthiness that neither our government nor the private sector alone is equipped to provide.[7] This landscape offers adversaries unique instruments of coercion, sabotage, espionage, and extortion used for digital, economic, and social overmatch.

The power and reach of cyber operations are growing, and other nations or nonstate actors can pressure the United States without committing military force or declaring their intent. The Interim National Security Strategic Guidance describes this landscape as a "revolution in technology that poses both peril and promise"—a race by global powers to develop and deploy emergent technologies.[8] The Joint Operating Environment 2035 describes the future of science, technology, and engineering as the means to reach technological parity and the ways that allow adversaries to challenge U.S. interests.[9] Warfare in 2035 will be defined by the use of force to disrupt global commons and a contest for cyberspace. The Joint Concept for Operating in the Information Environment refines a central theme to address this challenge and achieve enduring strategic outcomes.[10]

To succeed, the joint force must build cyberspace into operational art to design operations that deliberately leverage the informational aspects of military activities.[11] Leaders must understand cyberspace and informational aspects of military activities and informational power, defined as to "acquire, process, distribute, and employ data to enhance combat power."[12] This understanding requires the Services to integrate physical and informational power into training

Airman 1st Class Aden Gonzales of 83rd Network Operations Squadron participates in 688th Cyberspace Wing's 4th annual tactical-level exercise "Savage Cerberus 23," in San Antonio, Texas, May 12, 2023 (DOD/Nadine Wiley De Moura) and education pipelines, preparing cyber leaders as multidomain warriors. Innovation and the consistent integration of informational power in operational situations would provide commanders with a broader range of options that maximize military power.[13] The role of cyber leaders within this environment demands cognitive dedication to the fluid environment and its integration across all domains. Our current education of senior cyber leaders at Service war colleges must deliver on this demand signal.

Where We Stand Today. The Cyberspace Solarium clearly stated that the U.S. Government is poorly positioned to lead in cyberspace with the speed and agility needed to secure its interest.[14] The Solarium report suggests the government is weighed down by industrial-age bureaucracy, laws, and norms.[15] The insufficient number of cyber professionals in Federal service is hampering national efforts, and the report cites over 33,000 unfilled cyberspace positions in the U.S. Government.[16]

Difficulties in recruiting and retaining cyber talent are also impacting the Services. Retaining and developing personnel who employ cyberspace tools are so pivotal that the fiscal year 2022 (FY22) NDAA calls for DOD to assess its current cyber and information warfare curriculum across the joint education apparatus. The NDAA explicitly directs DOD to assess whether its current senior-level schools have the right curriculum and are the appropriate institutions for its delivery.[17] A new strategic posture is needed to position cyberspace as a warfighting domain with a commanding view of this rapidly evolving landscape.

The Solarium's key recommendation centered on the human capital dimension. Recommendation 1.5 states that the United States needs to recruit, develop, and retain a cyber workforce capable of building a defensible ecosystem and enabling the agile, effective deployment of all tools of national power in cyberspace.[18] Specific to this recommendation is the reinforcement of the National Institute of Standards and Technology role and the use of its National Initiative on Cybersecurity Education (NICE) workforce framework nationwide. The framework is the foundation for describing the tasks, knowledge, and skills required to perform cybersecurity work. It is also the cornerstone that enables organizations to develop their workforce to perform cybersecurity work and helps them determine the appropriate learning activities to advance their knowledge and skills. Specifically, the NICE framework is the organizing principle for the current DOD requirement to develop the cyber workforce, especially senior cyber leaders.

Today, none of the Services provides a dedicated program, beyond optional concentration studies and online certifications taken separately from PME, to meet this obligation at the place where most senior uniformed and civilian cyber officers are deliberately developed—the Service war colleges.

Current DOD Requirements. A recent National Cyber Strategy (2018) stresses the development of a superior cybersecurity workforce as a security advantage. It further states that the United States will "fully develop the vast American talent pool, while at the same time attracting the best and brightest among those abroad who share our values."[19] The strategy emphasizes that the Federal Government must use the NICE framework to standardize identifying, hiring, developing, and retaining a talented cybersecurity workforce. Success in the cyber domain will depend on the DOD ability to cultivate a high-quality workforce and develop leaders who can integrate new capabilities and adopt emergent approaches. At the time of its publication, there was no holistic DOD guidance that specifically addressed the scope of the cyberspace workforce beyond the information assurance sector.

So how does DOD develop its cyber talent and align with the NICE framework? Focus area one of the DOD cyberspace workforce strategy establishes a cohesive set of DOD-wide cyberspace workforce management issuances, the DOD 8140 publications. These publications address the demand to reevaluate staffing requirements, realign personnel within cyberspace work roles (codified in the DCWF), and retain qualified personnel. In cooperation with U.S. Cyber Command, DOD integrated a complete set of cyberspace work roles and qualification requirements into the overarching DCWF. The DOD 8140 publications are broken into the following three interrelated directives, instructions, and manuals:[20]

- DOD Directive 8140.01, *Cyberspace Workforce Management* (signed October 5, 2020)
  - authorizes the DOD Cyberspace Workforce Management Board
  - establishes elements in the cyber workforce
  - identifies roles and responsibilities within DOD
  - defines the cyberspace workforce.
- DOD Instruction 8140.02, *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements* (signed December 21, 2021)
  - offers guidance for identification, tracking, and reporting of DCWF work roles
  - identifies military and civilian requirements
  - provides the foundation for developing enterprise baseline cyberspace workforce qualifications.
- DOD Manual 8140.03, *Cyberspace Workforce Qualification and Management Program* (signed February 15, 2023)
  - assigns responsibilities and procedures for qualification of the cyberspace workforce
  - describes foundational (knowledge), residential (capability), and continuous development/qualification requirements
  - includes military, civilian, and contracted personnel.

The DOD 8140 publications address the full spectrum of the cyber workforce. The cyberspace workforce comprises personnel who build, secure, operate, defend, and protect DOD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace.

The DCWF represents a comprehensive standardized way to describe DOD cyber work with the intent to get the right people in the right positions. This framework allows Services to identify, track, and report cyberspace workforce personnel and their qualifications as required by the Federal Cybersecurity Workforce Assessment Act of 2015. The forthcoming DOD 8140 manual will list tasks and knowledge, skills, and abilities (KSAs) for 54 work roles within the DCWF. The DCWF features 54 work roles across 5 areas:

- cyber IT
- cybersecurity
- cyber effects
- cyber intelligence
- cyber enablers.[21]

Though the cyber leader work role is of great importance, future senior civilians and O6s may find themselves in the cyber policy and strategy planner role or any acquisition and project management role in support of major cyber and technology initiatives. Recently, the DCWF has been updated through a process known as DCWF Refresh and is codifying even more cyber leader roles for data and artificial intelligence.[22] These work roles are given three-digit codes, commonly referred to as "cyber coding."

Per DOD 8140 publications, cyber coding is intended to help identify, track, and report qualifications for personnel who perform cyberspace work roles using the authoritative personnel and manpower databases. The established codes will denote the work performed and corresponding proficiency level. This effort is ongoing, and the Services have achieved only the initial coding of the workforce. In 2021, over 120,000 military and civilian positions in DOD were cyber coded—and that does not count the military positions in the Army, U.S. Cyber Command, and a couple of others that were still working on completing military coding via their manpower systems.[23] Despite the missing data, the report is a good indicator of the size of the cyberspace workforce across DOD.

The DCWF and its cyber coding effort represent the DOD requirement to standardize cyber workforce management. Each cyber work role has a definition, a list of core and additional tasks, and KSAs that describe what is needed to execute critical functions and measure proficiency.[24] Cyber leaders are not exempt from the requirement. Extrapolating from the same DOD cyber coding report, the breakout of cyber positions coded as an "executive cyber leader" represents over 700 positions. The Army data, once complete, will raise those numbers considerably. The demand signal to ensure senior cyber leaders are fully qualified per DOD 8140 publications is apparent. Even without the final Army coding numbers, this represents a diverse and expanding number of senior cyber leader positions across DOD. Furthermore, in addition to using the DCWF to manage cyber workforce development and performance, the Services are directed to confirm compliance as an element of mission readiness.[25] The current apparatus for DOD leader development, joint PME, is tailored to meet this challenge.

Joint Education and Cyber. Joint PME is continuously refining the art and science of warfighting, particularly embracing technology and its integration to achieve mission success. The 2020 Joint Chiefs of Staff (JCS) vision and guidance for PME elaborates that changes in the character and conduct of war demand "continuous integration of national instruments of power and influence in support of national objectives . . . [and] a deeper understanding of the implications of disruptive and future technologies for adversaries and ourselves."[26]

Today's environment requires critical study of the information instrument of power, requisite cyber capabilities, and evolving technologies. To that end, the JCS vision lays out clearly that PME programs must provide graduates the knowledge and skills to prepare them for service as joint warfighting leaders, senior staff officers, and strategists who "anticipate and lead rapid adaptation and innovation during a dynamic period of acceleration in the rate of change in warfare under the conditions of Great Power competition and disruptive technology."[27] The DOD chief information officer (CIO) further echoes this task in his lines of effort (LOE) to meet the DOD Cyber Strategy. Of note is LOE 8—sustain a cyber workforce. This LOE has a specific objective to enhance the quality of the cyber education continuum across DOD. The LOE's relevant subobjectives include:

- 8-5-2: Enhance the cyberspace curriculum at joint PME schools by incorporating realistic and relevant case studies
- 8-5-3: Develop the concept for establishing a leadership-level cyber strategy development and planning framework into course curriculum at joint and Service-sponsored function courses
- 8-5-4: Incorporate cyber mission, roles, and responsibilities into required leadership training plans and curriculum.[28]

For the Service war colleges to execute this intent, their vector must coincide with the Chairman of the Joint Chiefs of Staff instruction on officer PME. The May 2020 release describes an outcomes-based approach across six joint learning areas (JLAs). The intent of the national and joint cyber visions and the DOD CIO LOEs can be translated across three of the six JLAs:

- JLA 3: The Continuum of Competition, Conflict, and War. The instruction describes joint leaders who use their knowledge of the nature and character of war to determine the challenges to U.S. national interests, evaluating the best use of the military instrument of power to achieve national security objectives.[29] Cyber technology contributes significantly to the evolution of war and global competition. Senior cyber leaders must shape the transition from the current cyber posture to a posture suited for the changing character of war. DOD Cyber Strategy LOE 8-5-2 is perfectly matched and can be met by this JLA.
- JLA 4: The Security Environment. The instruction describes the evaluation of innovative and technological

Marine Corps Corporal Joshua Mackaman, cyberspace warfare operator with Defensive Cyberspace Operations, Force Headquarters Group, Marine Forces Reserve, helps civilian with computer network analysis hacking game called "Packet Inspector" at DEF CON 31, Las Vegas, Nevada, August 11, 2023 (U.S. Marine Corps/Jonathan L. Gonzalez)

forces that pose threats, opportunities, and risks.[30] Senior cyber leaders are entrusted to lead and advise on cyber threats and opportunities. DOD Cyber Strategy LOE 8-5-2 and 8-5-4 can both be supported by this JLA because senior cyber leaders must understand their role in tackling the evolving security environment.

- JLA 5: Strategy and Joint Planning. The instruction describes joint officers who design all-domain plans across the spectrum of conflict.[31] Cyber is a warfighting domain per the numerous national and joint strategies previously discussed. Senior cyber leaders must account for this domain in all phases of planning. DOD Cyber Strategy LOE 8-5-3 fits in and can be met by this JLA because the cyber domain permeates strategy, operations, and tactics in all other domains.

The Chairman's instruction lists the National Defense University's College of Information and Cyberspace (CIC) as the only institution educating senior leaders in the cyberspace domain. This exclusivity matches neither the evolving security environment nor the cyber workforce per the DOD 8140 publications and recent coding data. The cyber domain has grown exponentially and, as noted before, permeates strategy, operations, and tactics in all domains.[32] Cyberspace cannot be taught at only one location for those few who were selected to attend CIC. Based on the 2021 RAND study, DOD covers an estimated 62 percent of the estimated yearly military demand for joint PME (JPME) II, resulting in officers in cyber and information roles likely to receive only general PME.[33] CIC is a modest, at best, proportion of the JPME II graduate population. To date, the U.S. Army War College, Air University, and Naval War College do not have a dedicated track to develop cyber leaders. By leveraging the JLAs, every Service war college can help meet the requirement to deliberately develop senior cyber leaders per the DOD cyber strategy and inform the DOD response to the FY22 NDAA assessment of cyber education at the Service war colleges. Cyber topics integrated into the general JPME II curriculum are no longer sufficient.

What Is a Cyber Leader? Recommendations

To adapt senior-level PME to meet the intent of the requirements established in national policy documents and framed in the DOD 8140 publications, the cyber leader work role must be defined. The current DCWF cyber leader work role summary is the foundation for the proposed recommendations. That is, the cyber leader executes decisionmaking authorities and establishes vision and direction for an organization's cyber and cyber-related policies, resources, and/or operations while maintaining responsibility for risk-related decisions affecting mission success.

A synthesis of the available KSAs for Federal cyber leader work roles and the recent CIC learning outcomes helps establish a baseline for the proposed cyberspace strategic studies track.[34] The following are recommended learning outcomes for this proposed track:

- evaluate the national security environment with an emphasis on the effect of cyberspace operations and related evolving technologies on all instruments of national power
- integrate joint doctrine perspectives into cyberspace operations and strategy
- analyze the critical aspects of cyberspace operations, technology, theories, laws, and policies in the development of national and Service strategies, joint operations, and other DOD activities
- evaluate and mitigate potential vulnerabilities of cyber capabilities, applications, and innovative and technological forces that pose threats, opportunities, and risks to joint operations
- apply principles of strategic leadership, decisionmaking, and ethical conduct regarding cyber capability employment.

As with any educational program, the challenge is to balance breadth and depth of knowledge. These learning outcomes set a path for success in balancing, on the one hand, the complementary set of essential KSAs to develop and defend the cyber environment with, on the other hand, strategic leadership underpinnings to influence departmental culture and military strategy.

This recommendation could be implemented with the help of the cyber resources and experts each Service has at its various educational institutions. Additionally, this recommendation positions CIC to reinvigorate its role as a "center of excellence" and support curriculum development, research opportunities, and Service war college partners—another shared conclusion with the RAND study.[35] The recommendation is both broad enough to allow for flexible implementation and detailed enough to allow for rapid implementation. There is no intent to swap or remove from an already crowded Joint Staff–directed curricula, only to use it as the foundational block in a dedicated track to narrow the focus on cyberspace and information. It parallels existing space, maritime, national security, and other differentiated tracks and shares the same intent: to prepare senior leaders in those areas demanding differentiated deliberate development.

The first step is establishing (or reestablishing) a cyber lead at each Service war college. This senior cyber leader will be a prominent on-staff advocate for cyber domain education while championing learning outcomes for senior cyber leaders, helping graduates meet DCWF cyber leader work role qualifications, and collaborating with intra-Service and inter-Service cyberspace educators. This track should include officers and civilians from cyber, information, space, acquisition, and information technology occupational specialties to bring in varying perspectives and prepare the full range of senior cyber leaders coded as such in the DCWF. This specialized track builds on the war colleges' current joint strategy and leadership curriculum by adding the unique perspectives and challenges cyberspace and information warfare present. It adds the origins of the cyberspace operational environment and national and DOD cyber strategies. It also seeks to incorporate curriculum on cyber technological capabilities, laws, policies, and data analytics. This could potentially include short trips to Service, DOD, and Department of Homeland Security cyber operations facilities, research laboratories, and industry partners. These trips and collaborative sessions with industry partners and other Federal agencies would prepare students to meet the NDAA requirement of expanded engagement outside DOD to explore different cyber capabilities and methods.[36]

Students in this track who are required by their Services to present research papers will focus on cyber and information domain challenges. The specialized track prepares students to provide cyber analysis and expertise during wargaming exercises, based on each of the war colleges' curricula. The proposed course essentials for the cyber strategic studies track are depicted in the figure and require further refinement from Service cyber institutions as well as recommendations from CIC. Adopting this recommendation ensures all learning objectives are met, and graduates will meet the DCWF Service requirements for the cyber leader work role.

Conclusion

Cyberspace has increasingly changed the way that war and global competition have evolved. The digital environment, initially designed to expand ideas and interaction, is now being used to circumvent U.S. sovereignty across all instruments of national power. It is an understatement to claim the introduction of cyberspace as a domain has had disruptive effects across the rest of the warfighting domains. Carl von Clausewitz warned that "all planning, particularly strategic planning, must pay attention to the character of contemporary war."[37] French academic and martyred World War II partisan Marc Bloch wrote of "theorists who were bogged down in errors engendered by the faulty teaching of history" and "the smell of decay rising from the Staff College," providing a harsh bridge from Clausewitz to modern criticisms from senior DOD officials.[38] DOD must adapt and innovate or find itself reacting to more attentive and agile actors.

The DOD cyber strategy LOEs and the 8140 publications set out the requirement to establish governance and structure for management of the cyber workforce and provide the foundation for qualification and development. Paramount to this effort is the development of joint senior cyber leaders. This is so critical that the DCWF designated a specific cyber leader work role. Leaders set culture, and we must ensure senior cyber leaders are fluent in the technologies, risks, and strategic cyber applications across all domains. Service war colleges are positioned to lead the DOD effort to develop senior cyber leaders to meet directives and find solutions that could develop each new generation of cyberspace leaders to succeed in this transformational warfighting domain.

To accelerate the transition from the force we have to the one required to win in cyber competition and conflict, the joint force must look beyond the rapid acquisition of ships, tanks, and planes. It must demonstrate an unwavering and growing commitment to deliberately developing senior cyber leaders who will shape this warfighting domain that permeates strategic, operational, and tactical levels in all other domains. Service war colleges can lead the way by pathfinding a dedicated cyberspace strategic studies track. **JFQ**

Thanks to Colonel Mark D. Coggins, USAF, Ph.D., Dr. Carl J. Horn, and Professor Gene C. Kamena from the Air War College for their thoughtful comments and suggestions regarding themes and ideas for this article.

Notes

[1] Angus King and Michael Gallagher, co-chairs, *Cyberspace Solarium Commission Report* (Washington, DC: U.S. Cyberspace Solarium Commission, March 2020), 8, https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf.

[2] Ibid., 1.

[3] Ibid.

[4] *Summary: Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, 2018), 5, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[5] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73 (2nd Quarter 2014), 14, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-73/Article/577499/the-joint-force-commanders-guide-to-cyberspace-operations/.

[6] Quentin E. Hodgson et al., *Educating for Evolving Operational Domains: Cyber and Information Education in the Department of Defense and the Role of the College of Information and Cyberspace* (Santa Monica, CA: RAND, 2022), iii, https://doi.org/10.7249/RRA1548-1.

[7] *Cyberspace Solarium Commission Report*, 1.

[8] *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 8, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[9] *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, July 14, 2016), 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.

[10] *Joint Concept for Operating in the Information Environment* (Washington, DC: The Joint Staff, July 25, 2018), 8, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

[11] Ibid.

[12] Ibid., viii.

[13] Ibid., 9.

[14] *Cyberspace Solarium Commission Report*, 16.

[15] Ibid., 15.

[16] Ibid., 16.

[17] National Defense Authorization Act for Fiscal Year 2022 (NDAA FY22), Pub. Law 117-81, 117th Cong., 1st sess. (December 27, 2021), 489.

[18] *Cyberspace Solarium Commission Report*, 43.

[19] *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 17, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[20] William Hess and Alfredo Rodriguez III, "USMC DOD 8140 OPT Presentation," USMC DOD 8140 Working Group, Headquarters Marine Corps, Washington, DC, June 14, 2021, 4.

[21] "DOD CIO Cyber Workforce Management," Defense Workforce Council presentation, Pentagon, Washington, DC, August 2021, 3.

[22] "DOD CIO Cyber Workforce News," *Defense.gov*, October 2020, https://dodcio.defense.gov/Portals/0/Documents/Cyber/WorkforceNewsletterOctober2020.pdf.

[23] Patrick Johnson, chief, Workforce Management Directorate, DOD-CIO, email to author, October 7, 2021; Department of Defense Inspector General (IG), *Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce (DODIG-2021-110)* (Washington, DC: Government Publishing Office, August 2, 2021), i, 2, 8, 11–12, 26, 28. The IG report redacted the numbers. Mr. Johnson provided releasable numbers in the email.

[24] Department of Defense Instruction 8140.02, *Identification, Tracking, and Reporting of the Cyberspace Workforce Requirements* (Washington, DC: Department of Defense, December 21, 2021), 9.

[25] Ibid., 6.

[26] *Developing Today's Joint Officers for Tomorrow's Ways of War: The Joint Chiefs of Staff Vision and Guidance for Professional Military Education and Talent Management* (Washington, DC: The Joint Staff, May 1, 2020), 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817.

[27] Ibid., 4.

[28] "DOD CIO Cyberspace Strategy Lines of Effort, LOE 8 Summary," Department of Defense CIO, October 4, 2019, 3.

[29] Chairman of the Joint Chiefs of Staff Instruction 1800.01F, *Officer Professional Military Education Policy* (Washington, DC: The Joint Staff, May 15, 2020), 26.

[30] Ibid., 25.

[31] Ibid.

[32] Joshua A. Sipper, "It's Not Just About Cyber Anymore: Multidisciplinary Cyber Education and Training Under the New Information Paradigm," *Joint Force Quarterly* 100 (1st Quarter 2021), 53, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497154/its-not-just-about-cyber-anymore-multidisciplinary-cyber-education-and-training/.

[33] Hodgson et al., *Educating for Evolving Operational Domains*, 28.

[34] Carl J. Horn, "College of Information and Cyberspace Update," National Defense University, August 7, 2019, 6.

[35] Hodgson et al., *Educating for Evolving Operational Domains*, 37.

[36] NDAA FY22, 492.

[37] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 220.

[38] Marc Bloch, *Strange Defeat: A Statement of Evidence Written in 1940* (New York: Norton, 1999), 125.

An Interview with Anthony J. Cotton

Joint Force Quarterly: *As the commander of U.S. Strategic Command* [USSTRATCOM], *how do you view the threats and challenges your command faces?*

General Anthony J. Cotton: Our threats are not isolated to one command or nation. These global challenges require a concerted effort to strengthen not only deterrence but also partnerships with our allies and partners. For the first time, the United States faces two major nuclear powers that could operate at any level or domain of conflict to meet their national objectives. We are now in a multipolar world with potential adversaries that could threaten the United States, our allies, and our partners with nuclear weapons and nonnuclear capabilities that could have devastating impacts.

The National Defense Strategy is clear that the most comprehensive and serious challenge to U.S. national security is the PRC [People's Republic of China]'s coercive and increasingly aggressive endeavor to refashion the Indo-Pacific region and the international system to suit its interests and authoritarian preferences. The PRC is the most serious challenge to U.S. national security holistically. We have seen incredible growth in China's nuclear arsenal, and it shows no signs of slowing down. It has a bona fide nuclear triad, and its increasingly provocative rhetoric and coercive activity in the Indo-Pacific region threaten a free and open Indo-Pacific.

But it is not just a matter of the PRC. Russia continues to present a strategic deterrence challenge, posing an immediate and persistent threat to international peace and stability. North Korea is also a growing concern. Although it doesn't have the capability or capacity of Russia or China, North Korea is expanding its nuclear capabilities and missile technology. It is also increasing its aggressive rhetoric and actions toward Japan, South Korea, and the United States.

Taken piece by piece, this situation is already a concern. But we must look at the whole and realize all three actors are increasing their levels of cooperation with one another. We recently saw China and Russia conduct a combined naval patrol that sailed near Alaska and the Aleutian Islands. We're also witnessing an expanding military partnership between Russia and the DPRK [Democratic People's Republic of Korea], where North Korea is agreeing to support Russia's war in Ukraine. These challenges will continue to grow and evolve and so will our capabilities. That's why integrated deterrence is so important; it brings together all military domains and instruments of power, along with those of our allies and partners, to deter the range of threats we face today and in the future.

General Anthony J. Cotton, USAF, is Commander of U.S. Strategic Command.

JFQ: *For many years during the Cold War, even during times of tension, the United States and Russia had a continuing dialogue on nuclear arms control, leading to several agreements that dramatically limited the numbers and types of nuclear weapons and delivery systems. How do you view the prospects for arms control agreements in the future, not only with New START but also with other states besides Russia?*

General Cotton: USSTRATCOM's mission is to reduce the risks of strategic attacks on the United States, its allies, and partners. I view arms control as a complementary effort, seeking the same objective by reducing the number of threats and enabling strategic stability dialogues with potential adversaries. Any arms control negotiations must address the reality of two major nuclear powers. As always, my command stands ready to support the Department of State.

JFQ: *The pressure of a growing range of threats from several states as well as non-state actors has led to questions about how the current triad of U.S. nuclear forces, first fielded in the Cold War, addresses this different world. Could you discuss how the modernization of U.S. nuclear forces might shape the international security environment in the future?*

General Cotton: It is important to state our legacy systems are safe, secure, effective, and credible. We're recapitalizing every leg of the nuclear triad and the corresponding nuclear command, control, and communications [NC3] architecture to ensure our continued ability to serve as a bedrock of national security. These long-term investments will ensure a predictable, stable, and efficient nuclear force for decades.

The B-21 Raider, Sentinel, our next-generation ICBM [intercontinental ballistic missile], the new *Columbia*-class ballistic missile submarine, B-52 commercial engine replacement program, AGM-181 Long-Range Standoff missile,

Airmen from 90th Maintenance Group maintain and repair intercontinental ballistic missiles on alert status, December 18, 2019, within Francis E. Warren Air Force Base, as part of Air Force Global Strike Command (U.S. Air Force/Abbigayle Williams)

Ohio-class ballistic missile submarine USS *Louisiana* transits Puget Sound following 41-month engineered refueling overhaul at Puget Sound Naval Shipyard and Intermediate Maintenance Facility, February 9, 2023 (U.S. Navy/Brian G. Reynolds)

and the next-generation nuclear command, control, and communication systems represent an era of significant transformation of U.S. nuclear forces. Our deterrence will only strengthen as we transition to these new systems that will be even more capable and synchronize our capabilities. The modernization of the nuclear triad, the weapons complex, and the infrastructure is critical to not only our nation's security but the security of our allies and partners as well.

JFQ: *Can you discuss the importance of the overall modernization effort and your ability to sustain support from the Services over the next decade to field those new systems, given the pressures each faces with other modernization requirements?*

General Cotton: Modernization is not a matter of "Can we?" It is a matter of "We must." Our nation's security, and the security of our allies and partners for whom we provide extended deterrence, depends on it. This is a once-in-a-generation evolution, so we're not just setting ourselves up for success; we are creating the new foundation for the next generation.

We're modernizing all legs of the triad at the same time. This includes resourcing, manpower, delivery, infrastructure, and support facilities. We are working with our Service partners to ensure alignment across the board, so our legacy systems remain effective as we transition into the modernized systems. We are spending an incredible amount of time to ensure we do not miss a step in the transition process. The Navy and Air Force are watching their efforts closely because they're the ones that present forces to me, which I present to the President, as required.

JFQ: *What is your assessment of USSTRATCOM's ability to gain and maintain situational awareness now that U.S. Space Command and U.S. Space Force have been established?*

General Cotton: The situational awareness of USSTRATCOM is strong due to the collaboration within the Department of Defense, specifically with U.S. Space Command and U.S. Space Force. For example, the Space Force's overhead persistent infrared satellites and ground-based radars provide strategic and theater missile warning. Combatant commands receive this information for awareness and conduct analysis and assessments to understand the strategic and tactical implications of space-related developments. Moreover, I look forward to the Next-Generation Overhead Persistent Infrared program, which will enhance our nation's situational awareness capabilities.

JFQ: *With the episodes of threats of nuclear weapons from Russia during its war on Ukraine and from the continuing missile launches from North Korea, how has your command worked with allies, partners, and neighboring states to reassure their governments of U.S. support to help reduce their defense concerns?*

General Cotton: Alliances and partnerships are key to protecting the rules-based international order. The strength of our alliances and partnerships gives us the asymmetric advantage that our competitors do not enjoy. For example, in 2023, we saw the first SSBN [ballistic missile submarine] port visit to South Korea in 40 years, an SSBN port visit to the United Kingdom, the first B-2 deployment to Iceland, a B-52 deployment to Indonesia, multiple bomber task force missions in the European and Indo-Pacific regions, and countless exercises. I believe these and other examples of assurance missions bolster our deterrence efforts around the world.

In addition to these operations, I recently had the opportunity to visit the Republic of Korea and Japan, where I met with senior military and government leaders to reaffirm, face-to-face, our commitment to extended deterrence.

We have liaison officers from Australia, Japan, the Republic of Korea, and the United Kingdom, all of whom work closely with us daily. It garners trust among alliances and creates relationships that are key to integration and collaboration.

JFQ: *Could you discuss the growing challenges of cyber threats and the ability to assure intelligence, surveillance, and reconnaissance information flows to support your forces and how the other combatant commands, particularly U.S. Cyber Command, help USSTRATCOM achieve situational awareness?*

General Cotton: Cybersecurity is not static. Adversaries and bad actors constantly evolve their practices, which is a continual concern. However, it goes back to the regular collaboration that happens at the combatant command level and at all levels in every Service. I speak with General [Paul M.] Nakasone [commander of U.S. Cyber Command, director of the National Security Agency/chief of the Central Security Service] regularly, and our J6 directorate, which maintains USSTRATCOM's command, control, communication, and computer systems. Also, our Nuclear Command, Control, and Communications Enterprise Center, which oversees the department's NC3 enterprise, works with U.S. Cyber Command often to ensure we remain ready and capable. Cybersecurity is interwoven in everything that we do.

JFQ: *Leadership at your level depends on the people who work for you. Given the various impacts of demographic trends in the United States and the frequent reports of shortages in qualified recruits for the Services, could you give us some of your insights into how you attract the military and civilian talent needed to meet your mission?*

General Cotton: Leadership at all levels, from the squadron to the combatant command, depends on a talented workforce. It is no secret that recruiting numbers are down, but America's military strength is built on a foundation of exceptional people—both military and civilian. Attracting talent to meet our nation's strategic deterrent mission is a top priority, and we continue taking steps to ensure we have the right force for the future.

We are engaging talent where they are—at think tanks, on college campuses, at military units around the world—and having conversations about the critical work being done at the command. We are reaching people at local job fairs, advertising available positions on our social media platforms, and directly hiring qualified personnel for specific roles. The Omaha area is a great place to live and work, so we routinely partner with local government, civic, and civilian leaders in the greater Omaha metro community to highlight how the area is a leader in quality of life and national security.

This year is the 50th anniversary of the all-volunteer force, and for 50 years, our nation has been in good hands, and we will continue to be in good hands. We have no option.

The men and women of USSTRATCOM are the foundation for the capabilities that underpin our nation's strategic deterrence, and they do this in an environment that continues to grow even more complex and challenging. If I issue an intent, the Soldiers, Marines, Sailors, Airmen, Guardians, and civilians within the nuclear enterprise will complete the mission. The reason I know that is due to the extraordinary leaders we have. From the most junior to the most senior, I trust all of them in their abilities to execute.

We are all ambassadors of the military, the command, and the mission. In that sense, we are all recruiters, so the shortfall is on us. We need engaged, skilled, and dedicated people to continue to join the nuclear enterprise, so it is clear we need to share our experiences. It is a matter of getting out in our communities, talking with our peers in the Services, and explaining the what and why of the mission—and why Omaha, Nebraska, is such a great place to serve. **JFQ**

China's People's Liberation Army Rocket Force during military parade at Zhurihe Training Base in Inner Mongolia Autonomous Region, July 30, 2017 (Xinhua/Alamy/Wu Xiaoling)

Wicked Deterrence Challenge
The Changing Strategic Landscape

By Thomas Hammerle

> *The most pressing strategic challenge facing our vision is from powers that layer authoritarian governance with a revisionist foreign policy. It is their behavior that poses a challenge to international peace and stability—especially waging or preparing for wars of aggression, actively undermining the democratic political processes of other countries, leveraging technology and supply chains for coercion and repression, and exporting an illiberal model of international order. Many non-democracies join the world's democracies in forswearing these behaviors. Unfortunately, Russia and the People's Republic of China do not.*
>
> —National Security Strategy

Major Thomas Hammerle, USA, is a Strategic Intelligence Officer at U.S. Strategic Command.

The National Security Strategy of the United States laid out that the Nation is entering a decisive decade—not only for itself but also for the world.[1] The current era of strategic competition is characterized by the reemergence of a geopolitical contest between powerful states over the shape of the future global order. After World War II, the Allies established a rules-based international order rooted in cooperative values and predicated on a framework of diplomatic and economic rules, led and enforced by like-minded nations. This system has enabled decades of prosperity for all nations that have elected to participate, but it is now under stress by revisionist nations. The People's Republic of China (PRC), Russia, and North Korea are each intent on changing the international order to achieve their national ambitions.

The changing strategic environment has created a wicked deterrence challenge that will test the United States and its allies. These revisionist states are dissatisfied with the current international order because they see it as a threat to their own national objectives. Their ambitions pose a direct strategic challenge to the continued security of the United States and its allies because these nations are increasingly capable and willing to use force as a coercion mechanism. Russia is openly flouting international laws and norms—including its own commitment to the 1994 Budapest Memorandum—by invading Ukraine, violating its sovereignty and attempting to annex territory by force. China seeks to establish its own sphere of influence in the Pacific region that excludes the United States and Western influence while also attempting to resolve territorial disputes through coercion and threatening behavior. The most serious component of these strategic challenges for the United States is the modernization and expansion of both Russia's and the PRC's nuclear arsenals. For the first time in its history, the United States is simultaneously facing two adversarial nuclear peers whose aspirations directly challenge U.S. national values and threaten U.S. allies.

Wicked Deterrence Challenge

A *wicked problem* is one that is difficult to solve because of its complexity, incomplete and changing information, multiple stakeholders, competing and conflicting objectives, clash of cultures, or the unprecedented or novel nature of the situation.[2] Deterrence, by its very nature as a function of influence over leadership decisionmaking, is a wicked problem. Leadership decisionmaking can be impacted by numerous unique factors, making the application of deterrence strategy more art than science. As Keith Payne writes, "There are few, if any, universal constants in this regard; instead, there is a wide variety of operating factors, some seen, others unseen, that can vary greatly across time, place, and opponent, and may be decisive in determining if and how deterrence will function."[3]

The emergence of the multilateral strategic environment and the need to deter many nuclear actors simultaneously while continuing to assure allies require the United States to rethink its deterrence policy. How does deterrence policy need to adapt to address the changing multi-actor environment? To begin to answer this question, analysts must start with building an understanding of the strategic environment, including a deep understanding of individual nations and the specific leaders the United States seeks to deter. While this understanding will never be perfect, it will reduce ignorance and provide a basis for designing a tailored deterrence policy.

People's Republic of China

The PRC's meteoric rise has been motivated by its perceived need to restore its rightful place in the world order—to right the wrongs done to China during its so-called Century of Humiliation. While former Chinese leader Deng Xiaoping articulated the PRC's strategy as one of patience—the famous "hide and bide" strategy—current President Xi Jinping has abandoned this approach, instead seizing the opportunity to achieve his Chinese Dream of the "great rejuvenation of the Chinese nation."[4] However, Xi views the current world order as an unacceptable impediment to China's geopolitical ambitions and the United States as a direct threat to its national security.[5] The PRC views Western and particularly U.S. influence in the Pacific region as a violation of its right to act as the regional hegemon and an impediment to unification with Taiwan. Xi envisions China as the rightful preeminent Asian and global power. Xi's bolder, more confrontational strategy has provoked responses both from regional nations concerned about their sovereignty and security and global nations invested in the current rules-based international order.

The PRC has repositioned itself politically, economically, and militarily to better enable it to achieve its aspirations. The People's Liberation Army (PLA) has undertaken a holistic military modernization of both its conventional and nuclear capabilities. Modernization efforts have been under way for decades, but they have increased to an alarming pace under Xi's leadership. The PRC has sought to develop an ability to forcibly expel Western forces and ultimately to prohibit their reentry into the region for the purpose of securing its ambitions. Nuclear weapons forces are "a strategic pillar of China's great power status," the linchpin in excluding U.S. and Western interference, and ultimately serve as the backstop to achieving its ambitions.[6]

The PLA's rapid development of its nuclear arsenal is the fastest peacetime expansion of a nuclear arsenal the world has witnessed, going from just a few hundred weapons at the end of the Cold War era to a projected 1,500 by 2035 if its current pace continues unabated.[7] These developments will match, and in some areas qualitatively exceed, equivalency with the United States. Xi has stated that he believes a robust nuclear weapons program is critical to the PRC's ability to counter the United States in the Pacific region. To this end, the PRC is investing in and expanding the number of its land-, sea-, and air-based nuclear delivery platforms and constructing the infrastructure necessary to support this major expansion.[8]

The PRC's nuclear strategy has been relatively consistent since it first acquired nuclear weapons in 1964, relying on a minimum deterrence strategy made credible by a small nuclear arsenal capable of delivering a secure second strike. The PRC's declared no-first-use policy further reinforced this public commitment to maintaining a nonaggressive position. However, the PRC's rapid nuclear expansion calls into question whether the PLA is still committed to this strategy.[9] In his testimony before the House Armed Services Committee, General Anthony Cotton, commander of U.S. Strategic Command, articulated this point, stating, "The PRC's actions are wholly inconsistent with its long-professed policy of minimum deterrence."[10] The expansion of the PRC's nuclear arsenal opens myriad possibilities of ways it could adapt its strategy to both deter and coerce other nations. However, due to a lack of transparency and an unwillingness to engage in dialogue, it is unclear what the PRC's intentions are.[11]

The PRC's potential to change its nuclear strategy cannot be understated in the maturing global circumstances. PLA officers are writing publicly about the need to articulate conditions under which nuclear first use may be permissible or even desirable. These include exceptional scenarios such as conventional defeat threatening regime survival, conventional attack on a nuclear scale, or attacks on PLA strategic forces.[12] As a result, the durability of the PRC's long-honored no-first-use policy may soon be limited or deficient. While PRC debate surrounding this policy gets the most attention from strategists and policymakers, there is also debate surrounding its "sole purpose" policy, with PLA strategists debating the benefits of using nuclear weapons to deter conventional conflict.[13] The active debate in the PRC about changing its nuclear policy coupled with a lack of transparency and communication increases uncertainty and the potential for instability.

The discovery of 300 new potential intercontinental ballistic missile (ICBM) silos brought into sharp relief the extent of the PRC's nuclear modernization and expansion.[14] When complete, these silos will provide the PRC with persistent readiness and the ability to conduct extremely rapid launch sequences. In addition to investing in fixed silos, the PLA Rocket Force is investing in road mobiles and expanding the number of launchers and crews in each unit at an unprecedented rate.[15] The PLA Navy's six *Jin*-class ballistic missile submarines (SSBNs) rotate through near-continuous deployment equipped with JL-2 submarine-launched ballistic missiles (SLBMs), though this platform is vulnerable as it needs to enter the open Pacific in order to target the United States. However, the PLA Navy is building the Type 096 SSBN, which will carry the updated JL-3 SLBM capable of targeting the United States from Chinese littoral waters, significantly increasing the survivability of its sea-based deterrent.[16] Finally, the PLA Air Force is reestablishing its air leg with the updated H6-N bomber, which will complete a true regional triad. It is also developing a new strategic bomber, the H-20, but while specifications are still unknown, it is clear that the PRC is intent on obtaining a credible global triad.[17] Beyond a traditional triad, the PRC is developing additional capabilities such as hypersonic missiles, fractional orbital bombardment systems, and the Dong Feng-26 medium-range ballistic missile with both conventional and nuclear payloads that could be swapped quickly in the field.[18] While these capabilities are not novel, they all have the potential to be destabilizing.

At the same time the PRC is modernizing its nuclear capabilities, it is modernizing the command and control infrastructure to support it. Investments in ground-based large phased-array radars and the ability to detect ballistic missile launches with geostationary satellites have provided the PRC with a comprehensive early warning capability.[19] These capabilities make credible the PRC's desire to shift to a "launch on warning" nuclear posture, increasing the potential for miscalculation. The U.S.-China Economic and Security Review Commission detailed the risk with such a posture, stating that the "difficulties associated with learning to operate such a system could generate false alarms about nonexistent incoming nuclear attacks, potentially triggering a nuclear exchange between China and the United States."[20] The PRC's unwillingness to enter risk-reduction dialogues and complete refusal to enter arms control negotiations mean these risks are left unaddressed.

Russia

The challenges posed by Russia to the rules-based international order have been on full display since at least 2008, with Russia's invasion of Georgia, and again in 2022 when President Vladimir Putin began his "special military operation" in Ukraine to halt Kyiv's economic and cultural progress toward the West. Putin views the U.S.-backed rules-based international order as a threat to the Russian way of life. It is his intent to renew the *Russkiy Mir*, the Russian world, and restore Russian prestige and cultural and political influence in the vein of previous Russian empires.[21]

The current revisionist and irredentist narrative in Russia argues that Russia is a victim of U.S.-European hegemony and is besieged by North Atlantic Treaty Organization (NATO) expansion in its periphery, a direct threat to the goal of reestablishing the Russian world. The war in Ukraine is a direct result of this perceived threat. Non-NATO and non–European Union states with strong relationships with the West, in general, have been less susceptible or receptive to Russian influence, thereby diminishing Russia's status in its near abroad. At the prospect of further NATO enlargement, Putin felt threatened to the point of taking belligerent action. According to Dmitri Trenin, a member of Russia's Foreign and Defense Policy Council, "What Russia craves is respect. It does not want to be a junior partner—it wants to be an equal."[22]

Despite significant initial gains in Ukraine, the Russian war effort has endured countless tactical, operational, and strategic setbacks and has begun to show clear signs of devolution into a protracted slog reminiscent of the Korean War in the 1950s. A significant portion of Russia's conventional capability has been degraded and destroyed by the ongoing conflict in Ukraine, which could increase Putin's reliance on nuclear capabilities for Russia's defense. The continued use of nuclear saber-rattling by Putin and

H-6K strategic bomber of China's People's Liberation Army Air Force (Stocktrek Images, Inc./Alamy)

other Russian officials has effectively deterred Western intervention and heavily influenced the type of military assistance the West is willing to provide to Ukraine and undermined Ukrainian resistance.[23] As evidenced by steadily increasing economic and material support from NATO, the effectiveness of these nuclear threats is eroding. Putin's legitimate reliance on nuclear weapons, however, coupled with robust nuclear signaling should not be ignored or dismissed out of hand because Russia's nuclear weapons arsenal remains a significant existential threat to the United States and its allies throughout Europe and the Pacific region.

The capability and credibility of Russia's strategic and tactical nuclear forces make them a serious concern that cannot be ignored. Russia continues to invest substantial resources to expand and modernize its strategic and nonstrategic nuclear capabilities. Russia's modernization plan, which has been in the works for over a decade, includes improving each leg of its triad of nuclear delivery systems and developing new and novel nuclear capabilities. For example, the Sarmat is a new silo-based ICBM that will be capable of carrying up to 10 nuclear warheads.[24] Russia's strategic submarine fleet will include an entirely new *Dolgorukiy* class of SSBN submarines equipped with SS-N-32 Bulava nuclear ballistic missiles by 2028. The Tu-160M supersonic strategic bomber aircraft has extended range and is equipped with more capable onboard systems than previous iterations, and 10 are already in the field.[25] The modernization of the Russian nuclear force has increased the capability and credibility of Russia's nuclear triad.

In addition to modernizing its legacy systems, Russia is developing and improving its hypersonic and other novel delivery systems. These include new systems such as the Avangard hypersonic glide vehicle, the Kinzhal air-launched ballistic missile, and the Tsirkon land-attack cruise missile. Furthermore, Russia maintains over 2,000 non–treaty accountable—often referred to as tactical or nonstrategic—nuclear weapons that provide diverse and flexible use and deterrence options. In fact, it is this very threat of tactical nuclear weapons that has caused NATO nations to revitalize focus on both their conventional and nuclear capabilities to ensure that the Alliance possesses a credible deterrent.[26] Both Russia's strategic and tactical nuclear weapons are backed by a body of doctrine that explicitly lays out the conditions for nuclear use, including possible first use in response to threats to the "existence of the state."[27]

Since 1972, the relationship between the United States and the Soviet Union, later the Russian Federation, has been partially stabilized by a series of arms control agreements that provided mechanisms for building trust and reducing risk by allowing some strategic predictability in the relationship. For the first time in more than 40 years, U.S.-Russia relations lack the stabilizing guardrails of these arms control treaties. The last

Tu-160M strategic bomber of Russian Air Force flying over Russia (Stocktrek Images, Inc./Alamy)

remaining arms control treaty regulating U.S. and Russian strategic forces, New START, has suffered due to the U.S. support of Ukraine after the Russian invasion. Shortly afterward, Russia began refusing onsite inspections by U.S. personnel allowed by the treaty. Later, Russia "paused" its compliance with New START and has since refused to begin negotiations to extend or modify the agreement, which is set to expire in February 2026.[28] The expiration of strategic treaties with Russia will not only end self-imposed restraints, potentially spurring an arms race, but will also eliminate one of the most important conduits for communication between the United States and Russia and set conditions for dangerous miscommunication, misunderstanding, and miscalculation.

North Korea

North Korea has posed a consistent threat to the United States and its allies since the 1953 armistice. The nature of this threat has oscillated between moderate and acute but has remained consistently hostile. The persistence of the threat and more acute emerging challenges have unfortunately allowed some to become numb to the true severity and magnitude of what a conflict with North Korea could mean for the region and the United States. Conversely, North Korean leader Kim Jong Un does not waver in his focus on the United States as the perceived preeminent existential threat to his nation. To secure his power and protect his regime, Kim continues to invest in and grow North Korea's nuclear arsenal. The growth of North Korea's nuclear power goes beyond security. Jung H. Pak, a Fellow at the Brookings Institution, observed, "[Kim] has elevated and embedded nuclear weapons in both the popular consciousness and the ideological, physical, and cultural landscape, enshrining them in North Korea's constitution and has effectively linked them to the country's perception of prosperity."[29]

Along with advancing weapons development, North Korea has continued to advance its nuclear program, accelerating its testing program while refining its nuclear doctrine. North Korea enshrines its nuclear doctrine into law, the most recent update occurring in 2022 with the establishment of the State Policy and Nuclear Forces. This law served as an update to the 2013 Law on Consolidating Position of Nuclear Weapons State. While the 2022 law remains consistent with the earlier version in affirming the role of nuclear weapons in deterring aggression or responding if deterrence should fail, it also outlined the situations that could warrant a preemptive nuclear attack.[30] Most concerning, the 2022 North Korean law details the potential for an automatic nuclear response—often referred to as a "dead man's hand" mechanism—should military commanders be unable to communicate with

leadership in Pyongyang during a conflict. This severely complicates the deterrence and escalation management strategies of the United States and its allies.[31]

Doubts regarding the credibility of North Korea's nuclear capability should be discarded. Each successive underground nuclear test has produced a larger yield, with North Korea's last test in 2017 producing a yield of approximately 250 kilotons—10 times larger than the bomb used at Nagasaki in 1945.[32] Furthermore, North Korea's delivery systems continue to advance as the nation adheres to an aggressive testing schedule. In 2022, North Korea conducted nearly 100 missile tests, more than it had ever conducted.[33] North Korea is developing ICBMs capable of holding the United States at risk and several intermediate- and medium-range ballistic missiles capable of targeting South Korea and Japan. It is also pursuing an SLBM capability, which would increase the survivability of its deterrent.[34] Estimating the size of North Korea's nuclear arsenal is exceedingly difficult, as the regime is even less transparent than that of the PRC. That stated, North Korea is thought to have anywhere from 35 to 65 warheads today, with the ability to add up to 18 more warheads per year.[35] The international community should no longer consider Kim a proxy of the Chinese Communist Party or a buffer state puppet and must not ignore North Korea's unique national objectives.

Complexity in the Multi-Actor Strategic Environment

The PRC, Russia, and North Korea represent primary nuclear security concerns for the United States and its allies because of those states' abilities to threaten existentially and coerce effectively. In the developing multi-actor environment, U.S. relationships with each of these states do not happen in a vacuum. The strategic environment contains other nuclear weapons states, including U.S. allies the United Kingdom and France. India and Pakistan are de facto nuclear weapons states, as they are not signatories to the Nuclear Nonproliferation Treaty (NPT), nor are they recognized as sanctioned nuclear weapons states by the NPT, as they acquired their capability after 1970. There are also additional nations that may desire nuclear weapons—adversaries such as Iran.

For its part, the United States extends deterrence with its nuclear umbrella through collective defense treaties to the 31 (soon to be 32) nations of NATO, as well as Japan, South Korea, and Australia. Thus, the deterrent relationships are never bilateral, as is often misremembered about the Cold War era, but instead contain the security concerns of multiple actors. As numerous deterrence scholars have expressed, including

People's Liberation Army Rocket Force displays its intermediate-range ballistic missile Dong Feng-26 during military parade in front of Tiananmen Gate during military parade to celebrate 70th anniversary of People's Republic of China, in Beijing, October 1, 2019 (UPI/Alamy/Tom Walker)

Thérèse Delpech, this multi-actor strategic environment "may make a situation more unstable . . . as [multiple actors] introduce more variables" into deterrence strategies.[36] In U.S. deterrence efforts, each deterrence relationship must be tailored for each state or actor and must consider the nearly incalculable positions of allies and partners as well as cooperators, competitors, and adversaries.

Cooperation between the United States and its traditional allies remains strong and continues to grow. However, in the maturing multi-actor deterrence reality, there is increased cooperation between and among the historically fiercely independent PRC, Russia, and North Korea in instances where their strategic objectives align. These adversaries also have their own strategic deterrent relationships beyond those with the United States. China, India, and Pakistan form a deterrence triangle that features China's and Pakistan's increasing cooperation while both actively deterring India and each other. This makes the second- and third-order effects of strategic choices as critically important as any deliberate direct effort. Actions taken by the United States to assure an Indo-Pacific ally could inspire the PRC to adjust its deterrent strategy, which could trigger India to adjust its deterrent strategy, causing a ripple effect into its deterrent relationship with Pakistan. Understanding how the relationships of adversaries, allies, partners, and third parties are interrelated and connected is necessary to operate in the multi-actor strategic environment.

Conclusion

Deterrence has been the cornerstone of the National Security Strategy (NSS) of the United States since defense strategist Bernard Brodie declared, "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose."[37] As we traverse what the NSS has declared as a decisive decade, the nature of deterrence strategy is changing. The emergence of a multi-actor strategic environment with two nuclear-peer adversaries and numerous other proliferation challenges poses a truly wicked problem that requires a concerted effort to unravel. Given the complexity of the problem, the best that can honestly be expected is probably an increase of understanding and a reduction of uncertainty. This begins with understanding each unique adversary and the relationships that influence strategic decisionmaking with that state, and evaluating which circumstances can maintain a U.S. and allied advantage.

The PRC and Russia pose the greatest threat to the United States and its allies, but they are not the only threats. North Korea is growing its nuclear arsenal and lowering the threshold for nuclear use. In addition, how these adversaries interact with each other will further challenge deterrence strategies. As the national objectives of the PRC, Russia, and North Korea align, increased instances of cooperation, coordination, or (potentially) alliance may emerge. Finally, these relationships are not immune from the influence of other actors in the strategic environment. India and Pakistan can affect the Sino-American deterrence relationship and vice versa. The incompatible visions for the international order, conflict of values, and clash of cultures are the hallmarks of this decisive decade. The United States and allies must adapt deterrence strategies to these changing circumstances.

In 1966, in his Day of Affirmation Address to the University of Cape Town in South Africa, Robert F. Kennedy stated, "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."[38] Today, the United States and allies face another time of danger and uncertainty. While it is filled with wicked deterrence challenges, the United States and allies have a history of facing challenges with courage and creativity. Building a shared understanding of the challenge is the first step of meeting the challenges of this decade. JFQ

Notes

[1] *National Security Strategy* (Washington, DC: The White House, October 2022), 8.

[2] John C. Camillus, "Strategy as a Wicked Problem," *Harvard Business Review*, May 2008.

[3] Keith B. Payne, *Deterrence Is Not Rocket Science: It Is More Difficult*, Information Series, Issue No. 527 (Fairfax, VA: National Institute Press, July 6, 2022), https://nipp.org/wp-content/uploads/2022/07/IS-527.pdf.

[4] Jennifer Bradley, *China's Strategic Ambitions: A Strategy to Address China's Nuclear Breakout*, Information Series, Issue No. 531 (Fairfax, VA: National Institute Press, August 17, 2022), https://nipp.org/wp-content/uploads/2022/08/IS-531.pdf.

[5] Michael Beckley and Hal Brands, "The End of China's Rise," *Foreign Affairs*, October 1, 2021, https://www.foreignaffairs.com/articles/china/2021-10-01/end-chinas-rise.

[6] Zhao Tong, "What's Driving China's Nuclear Buildup?" Carnegie Endowment for International Peace, August 5, 2021, https://carnegieendowment.org/2021/08/05/what-s-driving-china-s-nuclear-buildup-pub-85106.

[7] Bonnie Denise Jenkins, "China's Military Modernization: Implications for Regional Security Track 1.5 Dialogue," Department of State, June 28, 2023, https://www.state.gov/keynote-remarks-for-chinas-military-modernization-implications-for-regional-security-track-1-5-dialogue/.

[8] "Statement of Anthony J. Cotton, Commander, United States Strategic Command, Before the House Armed Services Committee on Strategic Forces, March 8, 2023," https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/2023%20USSTRATCOM%20Congressional%20Posture%20Statement%20-%20HASC-SF.pdf; *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, February 6, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[9] Grant Van Robays et al., "A Great Nuclear Rejuvenation: What China Can Do With an Expanded Nuclear Arsenal," *Space and Defense Journal* 14, no. 1 (Spring 2023), 7–21, https://digitalcommons.unomaha.edu/spaceanddefense/vol14/iss1/1/.

[10] Cotton.

[11] Jennifer Bradley, *China's Nuclear Modernization and Expansion: Ways Beijing Could Adapt Its Nuclear Policy* (Fairfax, VA: National Institute Press, July 2022), https://nipp.org/wp-content/uploads/2022/07/Vol.-2-No.-7.pdf.

[12] Cotton; *Annual Threat Assessment of the U.S. Intelligence Community.*

[13] Bradley, *China's Nuclear Modernization and Expansion*, 27.

[14] Ashley Roque, "New Pentagon Report Details China's Growing Nuclear Arsenal, Possible New Missile Effort," *Breaking Defense*, October 19, 2023, https://breakingdefense.com/2023/10/new-pentagon-report-details-chinas-growing-nuclear-arsenal-possible-new-missile-effort/.

[15] *Military and Security Developments Involving the People's Republic of China 2023: Annual Report to Congress* (Washington, DC: Department of Defense, 2023), viii.

[16] Patty-Jane Geller and Peter Brooks, "China's Growing Nuclear Threat," Factsheet No. 209, Heritage Foundation, May 3, 2021, https://www.heritage.org/sites/default/files/2021-05/FS_209.pdf.

[17] Mark Episkopos, "Why China's Mysterious H-20 Bomber Could Be a Real Threat," The National Interest, May 26, 2021.

[18] Jenkins, *China's Military Modernization.*

[19] Ibid.

[20] *2021 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: Government Publishing Office, 2021), "Section 2: China's Nuclear Forces: Moving Beyond A Minimal Deterrent," 360, https://www.uscc.gov/sites/default/files/2021-11/2021_Annual_Report_to_Congress.pdf.

[21] Wilfried Jilge, "Russkiy Mir: 'Russian World'," German Council on Foreign Relations, May 3, 2016.

[22] Pierre Hassner, "Russia's Transition to Autocracy," *Journal of Democracy* 19, no. 2 (April 2008), 5–15, https://www.journalofdemocracy.org/articles/russias-transition-to-autocracy/.

[23] Pierre de Dreuzy and Andrea Gilli, "Russia's Nuclear Coercion in Ukraine," *NATO Review*, November 29, 2022, https://www.nato.int/docu/review/articles/2022/11/29/russias-nuclear-coercion-in-ukraine/index.html.

[24] Maxim Starchak, "Russia's Sarmat Missile Saga Reflects an Industry in Crisis," Carnegie Endowment for International Peace, October 18, 2023, https://carnegieendowment.org/politika/90795.

[25] Cotton; *Annual Threat Assessment of the U.S. Intelligence Community.*

[26] Dreuzy and Gilli, "Russia's Nuclear Coercion in Ukraine."

[27] Cotton; *Annual Threat Assessment of the U.S. Intelligence Community.*

[28] Frank G. Klotz and William Courtney, "Hard Times for U.S.-Russia Nuclear Arms Control," RAND, August 28, 2023.

[29] Jung H. Pak, "What Kim Wants: The Hopes and Fears of North Korea's Dictator," *Foreign Affairs*, May/June 2020.

[30] Bruce Klinger, *The Troubling New Changes to North Korea's Nuclear Doctrine*, Backgrounder No. 3729 (Washington, DC: Heritage Foundation, October 17, 2022), https://www.heritage.org/sites/default/files/2022-10/BG3729.pdf.

[31] Ibid.

[32] Bruce W. Bennett et al., *Countering the Risks of North Korean Nuclear Weapons* (Santa Monica, CA: RAND, April 2021), 27–28, https://www.rand.org/pubs/perspectives/PEA1015-1.html.

[33] Sue Mi Terry, "The New North Korean Threat: Why the United States Needs to Address Pyongyang's Nuclear Advances Now," *Foreign Affairs*, January 19, 2023, https://www.foreignaffairs.com/north-korea/new-north-korean-threat.

[34] "Nuclear Disarmament North Korea," Nuclear Threat Initiative, September 14, 2023.

[35] Bennett et al., *Countering the Risks of North Korean Nuclear Weapons*, 36–37.

[36] Thérèse Delpech, *Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Policy* (Santa Monica, CA: RAND, January 2012), 39, https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1103.pdf.

[37] "Brodie and the Bomb," *Air Force Magazine*, June 1, 2013, https://www.airandspaceforces.com/PDF/MagazineArchive/Documents/2013/June%202013/0613keeper.pdf.

[38] Robert F. Kennedy, "Day of Affirmation Address, University of Capetown, Capetown, South Africa, June 6, 1966," John F. Kennedy Presidential Library and Museum, https://www.jfklibrary.org/learn/about-jfk/the-kennedy-family/robert-f-kennedy/robert-f-kennedy-speeches/day-of-affirmation-address-university-of-capetown-capetown-south-africa-june-6-1966.

B-2 Spirit assigned to 509th Bomb Wing takes off from Joint Base Elmendorf-Richardson, Alaska, July 19, 2023, as part of bomber Agile Combat Employment exercise (U.S. Air Force/ Patrick Sullivan)

New Strategic Deterrence Frameworks for Modern-Day Challenges

By Kayse Jansen

Once again, the United States must contend with the prospect of conflict with a strategic adversary. In fact, the Nation must consider the potential for conflict with multiple strategic competitors that are all increasingly reliant on nuclear weapons to achieve their national objectives. Russia's enduring reliance on its nuclear arsenal and China's dramatic nuclear expansion mean that, for the first time in its history, the United States will soon face two nuclear peers. North Korea's accelerating nuclear capability further complicates an already challenging security environment. Even more alarming: All three potential adversaries are expanding the breadth and depth of their relationships and areas of cooperation.

Today's threat landscape stands in stark contrast to the profile of threats facing the United States and its allies just 10 years ago and is the catalyst driving bipartisan support for the Nation's wholesale nuclear recapitalization. Over the next 20 years or so, the Department of Defense

Kayse Jansen is Senior Technical Advisor in the Plans and Policy Directorate at U.S. Strategic Command.

(DOD) and the Department of Energy will replace every U.S. nuclear weapons system (except for the B-52, which is getting renovated); modernize the associated nuclear command, control, and communications architecture; and revitalize weapons production infrastructure. These efforts will ensure credible and effective forces for decades to come. Yet an often overlooked but equally important aspect of the enterprise requires the same level of focus and energy—intellectual capital.

Decades of fighting militarily inferior adversaries with little to no concern of strategic escalation have atrophied the intellectual frameworks required to deter and, if necessary, fight today's potential adversaries. Paths to nuclear use, strategies that simultaneously account for prevailing conventionally while deterring strategic attacks, and concepts to restore deterrence should an adversary choose strategic escalation are among the most important considerations the United States must contend with in an era of intensifying Great Power competition. So along with modernizing the hardware and software of the U.S. nuclear enterprise, we are called to revitalize our cognitive approaches. This requires the national security community to understand the character of today's security environment, revisit and refresh enduring deterrence truths, and explore new deterrence frameworks necessary for modern-day challenges.

A New and Complex Security Environment

"Deterring strategic attacks against the United States, Allies, and partners"[1] is one of the top DOD priorities. Adjectives preceding the word *deterrence* often evoke confusion, debate, and misinterpretation, so for the purposes of this article, *strategic deterrence* simply refers to deterring strategic attacks. Any use of nuclear weapons against the United States, its allies, or partners would be considered a "strategic attack," but not all potential strategic attacks involve the use of nuclear weapons. In fact, U.S. policy is intentionally vague in defining what constitutes a strategic attack. In large part, this is due to a necessary level of humility, realizing we might not know how to characterize a nonnuclear strategic attack until one occurs. Given the rapid advancements in technology and a dramatic increase in reliance on those technologies, there is a growing range of scenarios that could be strategic in nature but are not well understood today. Regardless of our ability to know these scenarios, the United States still seeks to deter their emergence.

Today's security environment is one of intense complexity. Such complexity stems not only from the myriad threats facing the United States and its allies and partners but also from the number of potential adversaries capable of carrying out those threats—that is, strategic competitors. Further complicating the issue is the growing cooperation between our strategic competitors centered on a common goal to upend and replace the liberal rules-based international order or simply minimize or eliminate U.S. influence in their near abroad. In short, we face a congested and compounding security environment.

Congested. U.S. relations with its strategic competitors are becoming increasingly strained. Individually, China, Russia, and North Korea are all capable of conducting strategic attacks against the United States or its allies and partners. Iran could also be classified as a strategic actor because of its regional missile capabilities. The "so what?" emerges when we connect the dots—that the potential for crises and armed conflicts is increasing for all strategic competitors. While simultaneously deterring all these actors is difficult, the challenge is more complicated.

Compounding. We can no longer consider potential adversaries *purely* as separate and distinct challenges that can be addressed via individually tailored strategies. As China, Russia, North Korea, and even Iran expand cooperation with one another, they are becoming increasingly united, at least in their proximate security objectives. There is building momentum in the global adversarial system that will continue to challenge the liberal rules-based international order. The result is a threat environment in which the collective actions of multiple strategic competitors maneuvering in coordination is more complex than confronting multiple strategic actors individually. Taken a step further, should simultaneous crises or conflicts develop, they will not be isolated events. At a minimum, U.S. actions and messages aimed at one will be seen and interpreted by others, but even this is insufficient to capture the compounding nature of the security environment. The risk of opportunistic escalation in those crises and conflicts, whether coordinated or otherwise, is growing. Stated differently, the decision calculus of a potential adversary regarding an escalation choice is likely influenced and potentially emboldened by the existence of other like-minded actors revolting against the status quo.

If the challenges of today's security environment are fundamentally more complex than in previous eras, what are the implications for deterrence? Which aspects of deterrence theory and practice still hold, and which require modernization? This article seeks to distinguish between the truths of deterrence theory that remain valid and worthy of review and the applications of that theory that must evolve to meet modern-day challenges. To that end, the article introduces new strategic deterrence frameworks with the goal of advancing efforts to develop holistic, multiactor strategic deterrence concepts fit for today's security environment.

Deterrence Foundations: Enduring Truths

Contemplating future deterrence strategies requires recalling basic deterrence principles that remain fit for purpose. These include the fundamentals of deterrence theory that have held since the advent of nuclear weapons, the nature of deterrence evolution across the spectrum of conflict that points to the relationship between deterrence and compellence, and the interplay between deterrence and other national security strategies such as competition and warfighting that can either be mutually supportive or in tension. While enduring, some truths have been skewed or simplified over the decades, so the Nation has not seriously considered them. Thus, the following sections not only reintroduce some of these truths but also emphasize nuances that have been diminished or dismissed during the time of U.S. unipolarity.

Deterrence Theory Fundamentals. *Deterrence* is an intentional act or set of actions aimed to influence adversaries' decisionmaking, so that adversaries choose restraint over aggression. Influence is directed at four factors of a decision calculus: costs of action, costs of restraint, benefits of action, and benefits of restraint. These costs and benefits are based on a decisionmaker's perceptions. With this being the case, effective deterrence relies on identifying and accurately evaluating aspects of an actor's strategic culture and vital interests, which influence its value judgments, risk-taking propensity, and myriad other factors shaping its decisionmaking processes. A common shortcoming of deterrence strategies is the tendency to project one's own values and ways of thinking onto the target, resulting in ineffective deterrence operations or misclassification of a potential adversary as irrational.

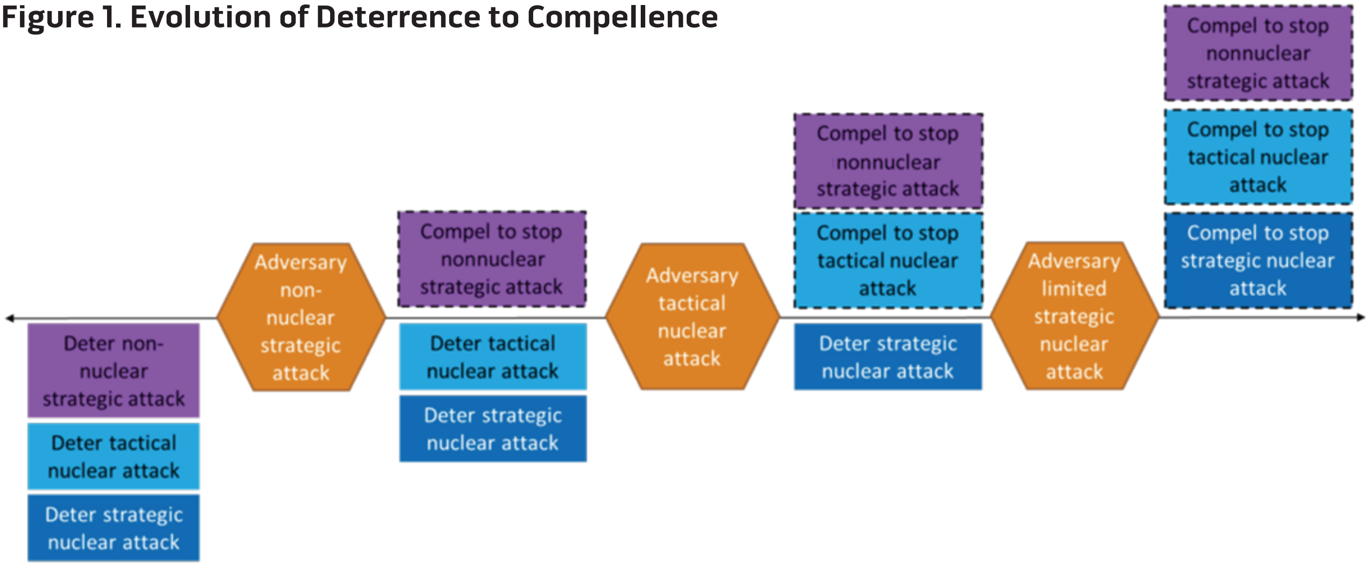
Deterrence strategies too narrowly focused on cost imposition (that is, influencing an adversary's perceived costs of action) and benefit denial (influencing an adversary's perceived benefits of action) may also be insufficient in effectively influencing a decision, especially when matters of national security are on the line. In such scenarios, a potential adversary's perceived costs of inaction (the consequences of doing nothing) are critical drivers of deterrence failure. If a decisionmaker is convinced that the costs of doing nothing are simply unacceptable, then it may very well risk incurring whatever costs an opponent has threatened to impose. Simply put, the certainty of the consequences facing an adversary if it does not act may outweigh the uncertainty of consequences if it does act.

Deterrence Across the Spectrum of Conflict. A second basic principle is that multiple deterrence objectives exist simultaneously and evolve in priority and nature according to the level of aggression in play. Simultaneous deterrence objectives include deterring aggression deterring armed conflict, deterring limited tactical nuclear use, deterring nonnuclear strategic attack, and deterring large-scale nuclear use. In peacetime, all these objectives exist, but those focused on higher levels of escalation are not as urgent because they are at a much lower risk of failure. Thus, while deterring strategic attack is always a U.S. objective, the risk of such an attack day to day is near zero, so activities and messaging are primarily aimed at deterring aggression that could lead to a crisis. A corollary to this principle is that deterrence does not fail all at once but in stages.

The nature of deterrence objectives also evolves. Should a deterrence objective fail, one seeks to restore it. If deterrence of armed conflict fails, one engages in operations, activities, and investments aimed at restoring that deterrence or, stated differently, compelling de-escalation and, ultimately, termination of the conflict. Thus, the nature of deterrence objectives, once overcome, evolves into a compellence objective (see figure 1). This is true even of deterring strategic attacks. Should an adversary conduct a strategic attack, nuclear or otherwise, the United States does not simply respond by escalating to the highest levels of nuclear use but responds in a way that seeks to restore deterrence of strategic attacks. The evolution of deterrence objectives will likely not be so linear—there are no laws of physics requiring a stair stepping (or ladder climbing) escalation path. But more on that later.

Deterrence and compellence are two sides of the same coin. Both rely on threats and promises to influence an adversary not to take an action or to stop aggressive actions.[2] I call this *deterrence-based influence* (DBI), from here forward used interchangeably with *deterrence.* Whereas deterrence approaches revolve around "if you do not, I will not" (that is, promise-based messaging regarding costs and benefits of restraint) and "if you do, I will" (threat-based messaging regarding

Figure 1. Evolution of Deterrence to Compellence


Deter non-nuclear strategic attack
Deter tactical nuclear attack
Deter strategic nuclear attack
Adversary non-nuclear strategic attack
Compel to stop nonnuclear strategic attack
Deter tactical nuclear attack
Deter strategic nuclear attack
Adversary tactical nuclear attack
Compel to stop nonnuclear strategic attack
Compel to stop tactical nuclear attack
Deter strategic nuclear attack
Adversary limited strategic nuclear attack
Compel to stop nonnuclear strategic attack
Compel to stop tactical nuclear attack
Compel to stop strategic nuclear attack

Ohio-class ballistic-missile submarine USS *West Virginia* conducts port visit at U.S. Navy Support Facility Diego Garcia during scheduled patrol, Diego Garcia, British Indian Ocean Territory, October 25, 2022 (U.S. Navy/Jan David De Luna Mercado)

costs and benefits of action), compellence centers on "if you do not stop, I will not stop" (threat-based messaging *and actions* regarding costs and benefits of action) and "if you stop, I will stop" (promise-based messaging *and actions* regarding costs and benefits of restraint). An influencer must be credible not only in its threats but also in its promises.

Deterrence—Competition—Warfighting. The final enduring principle is that deterrence, from the U.S. perspective, is not the same as competition or warfighting, or even preparation for warfighting. DBI depends on the adversary's point of view. Competition and warfighting center on one's own competencies, capabilities, and capacities. While typically assessed in comparison to a potential adversary's competencies, capabilities, and capacities, competition and warfighting sufficiency are ultimately determined by one's own perspectives, national goals, strategy, policy, and ways of warfare. This is why simply preparing for war is not a sufficient deterrence strategy. It considers only one's own perspective of readiness and, in doing so, addresses only half of a potential adversary's decision calculus via threats of cost imposition and benefit denial.

Competition activities and warfare preparation can, and often do, support deterrence by positively influencing an adversary's perceived costs and benefits of action. However, these activities can also undermine deterrence by negatively influencing an adversary's perceived costs and benefits of restraint. Competition activities may remove opportunities for collaboration, thereby removing any potential benefits of restraint. Competition activities may also undermine a potential adversary's vital national interests and its perceived security, thereby exacerbating potential costs of restraint. At the same time, activities geared toward warfare preparation may risk worsening perceived costs of restraint if they are perceived as closing a window of opportunity or are interpreted as offensive in nature rather than defensive.

Competition and warfare preparation, if unconstrained, risk undermining deterrence. Thus, it is critical that security strategies recognize and balance the interplay among deterrence, competition, and warfighting. As discussed in the next section, this interplay presents a dilemma in the day-to-day DBI period.

New Strategic Deterrence Frameworks

Modernized strategic deterrence frameworks are necessary to analyze and navigate a new and changing security environment characterized by increasingly aligned strategic competitors armed with a growing range of escalation options. The goal of introducing new frameworks is to equip the national security community with fresh ways to think about strategic deterrence and, ultimately, develop modern DBI concepts and strategies that address today's complex, congested, and compounding security environment.

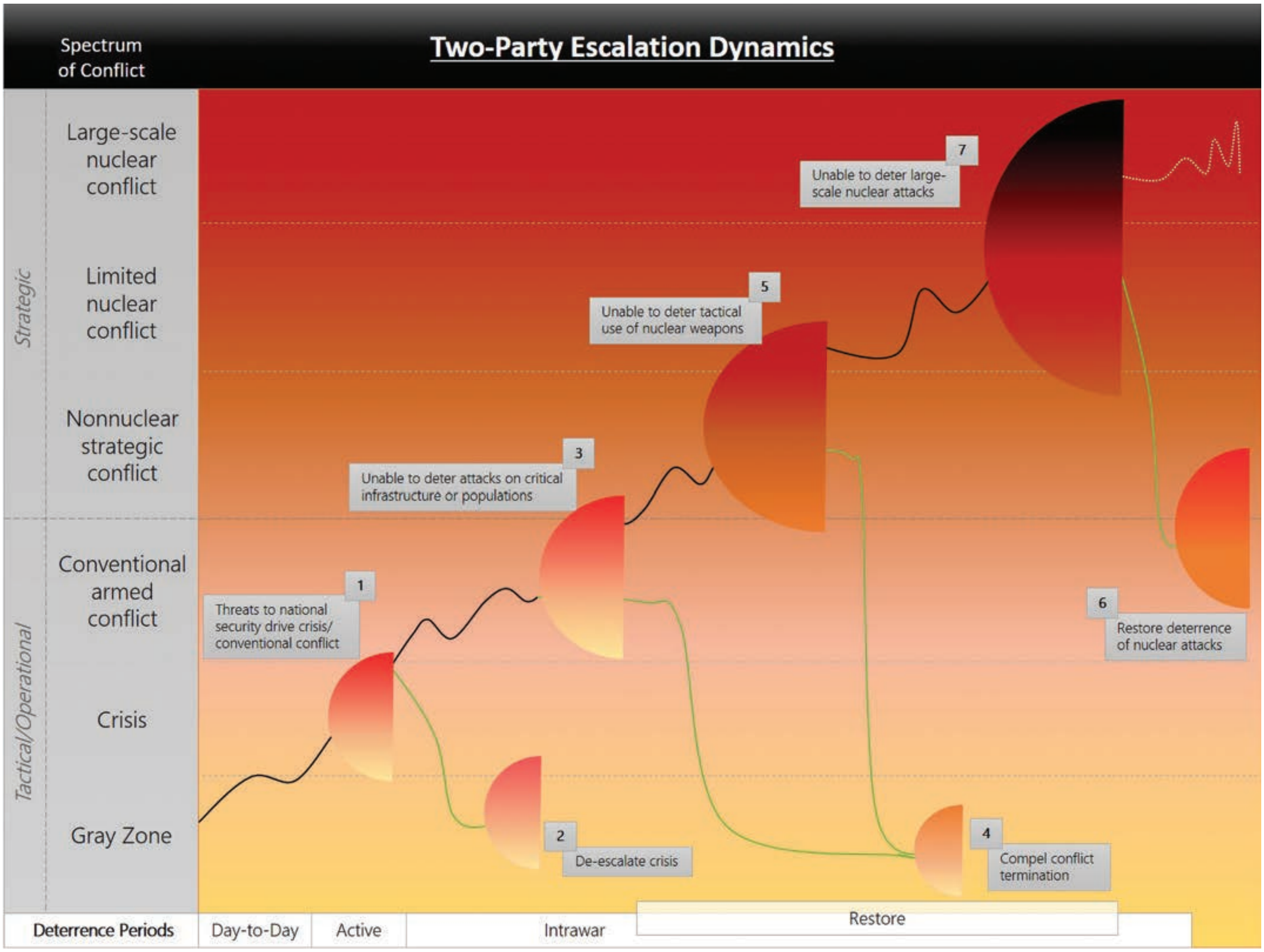
Escalation Dynamics. Developing effective deterrence strategies requires understanding the nature of escalation dynamics. When considering the potential for conflict with a strategic adversary, escalation dynamics are best characterized by chaos theory, where certain properties of a chaotic network (unfortunately) apply quite well.

First, a chaotic network is one in which the future state of a system is unpredictable. DBI relies on understanding an adversary's perceptions and is therefore already challenged by a high level of uncertainty. The challenge grows when seeking to understand, and then influence, perceptions in a crisis or conflict, when stress is elevated and the reality of not knowing the adversary's strategy or intent comes to fruition.

Uncertainty is a defining attribute of potential crisis or conflict with a strategic competitor; it was not a driving factor in the war on terror or other conflicts the Nation faced over the last few decades. Indeed, these battles contained their own complexities and challenges, but none of them risked escalation to a strategic level. Each adversary was constrained by its limited capacities and capabilities, and all were inferior to the United States and its allies and partners. The result was total domination on the battlefield with no concern of strategic escalation. This is not the case when considering conflict with a strategic adversary, where uncertainty exists across the entire spectrum of conflict and grows with each level of aggression. Uncertainty is depicted as cones in figure 2, distinct inflection points where the adversary can escalate at a time and place of its choosing (that is, points 1, 3, 5, and 7). Points 2, 4, and 6, along with their coordinating green off-ramps, depict U.S. attempts to de-escalate, or compel termination, of varying levels of aggression.

It is important to recall just how significant the concept of uncertainty is in the arena of strategic deterrence. Full-scale armed conflict between two nuclear-armed adversaries has no historical precedent. How such a conflict progresses, whether the capacity for nuclear use results in uncontrolled escalation or extreme restraint, is hypothetical. Thus, deterrence strategies must be flexible to a wide range of potentialities. Concepts such as "escalation management" or "escalation control" are outdated in this context. Rather, new concepts such as "escalation maneuver" are necessary to create a sense of adaptability to uncontrollable factors. Innovations in nonnuclear capabilities and growing reliance on space and cyber further exacerbate potential uncertainties, namely, the form that nonnuclear strategic attacks will take and the extent of their impact on populations and national decisionmakers.

Figure 2. Two-Party Escalation Dynamics


Spectrum of Conflict
Two-Party Escalation Dynamics
Strategic
Large-scale nuclear conflict
Limited nuclear conflict
Nonnuclear strategic conflict
Tactical/Operational
Conventional armed conflict
Crisis
Gray Zone
7
Unable to deter large-scale nuclear attacks
5
Unable to deter tactical use of nuclear weapons
3
Unable to deter attacks on critical infrastructure or populations
1
Threats to national security drive crisis/conventional conflict
2
De-escalate crisis
4
Compel conflict termination
6
Restore deterrence of nuclear attacks
Deterrence Periods
Day-to-Day
Active
Intrawar
Restore

Airman 1st Class Jackson Ligon, left, and Senior Airman Jonathan Marinaccio, 341st Missile Maintenance Squadron technicians, connect reentry system to spacer on intercontinental ballistic missile during simulated electronic launch Minuteman test, September 22, 2020, at launch facility near Great Falls, Montana (U.S. Air Force/Daniel Brosam)

The second attribute of a chaotic network is a sensitivity to initial conditions. In short, slight changes to system inputs can result in dramatically different futures. Applying this characteristic to escalation dynamics reveals that the entire spectrum of conflict is interconnected. Activities conducted today, and activities that occurred in the past, influence the path of escalation in the future or whether escalation occurs at all. As a result, strategists must consider the tradeoffs between taking risks now versus taking risks later. In some circumstances, it may be necessary to take provocative actions early, as the consequences of escalation are more acceptable in crisis than they would be in conflict. This is called *forward connectivity*, but there is also backward connectivity. *Backward connectivity* refers to the impact that future potentialities have on activities conducted today. This is not a new concept. During the Cold War, for instance, it was described as the *nuclear shadow*: the capacity of a nation to escalate to the highest levels of aggression both enables and restrains its behavior in every scenario short of that extreme. As a result, strategic deterrence is concerned not only with the potential of strategic attack but also the potential of a crisis or conflict in the first place, and even the nature of competition in the gray zone leading to a crisis. Furthermore, deterrence strategies must heed the way conflict is prosecuted, realizing the way in which the actor achieves objectives at the tactical/operational level influences an adversary's decision calculus regarding the need or opportunity to escalate to the strategic level.

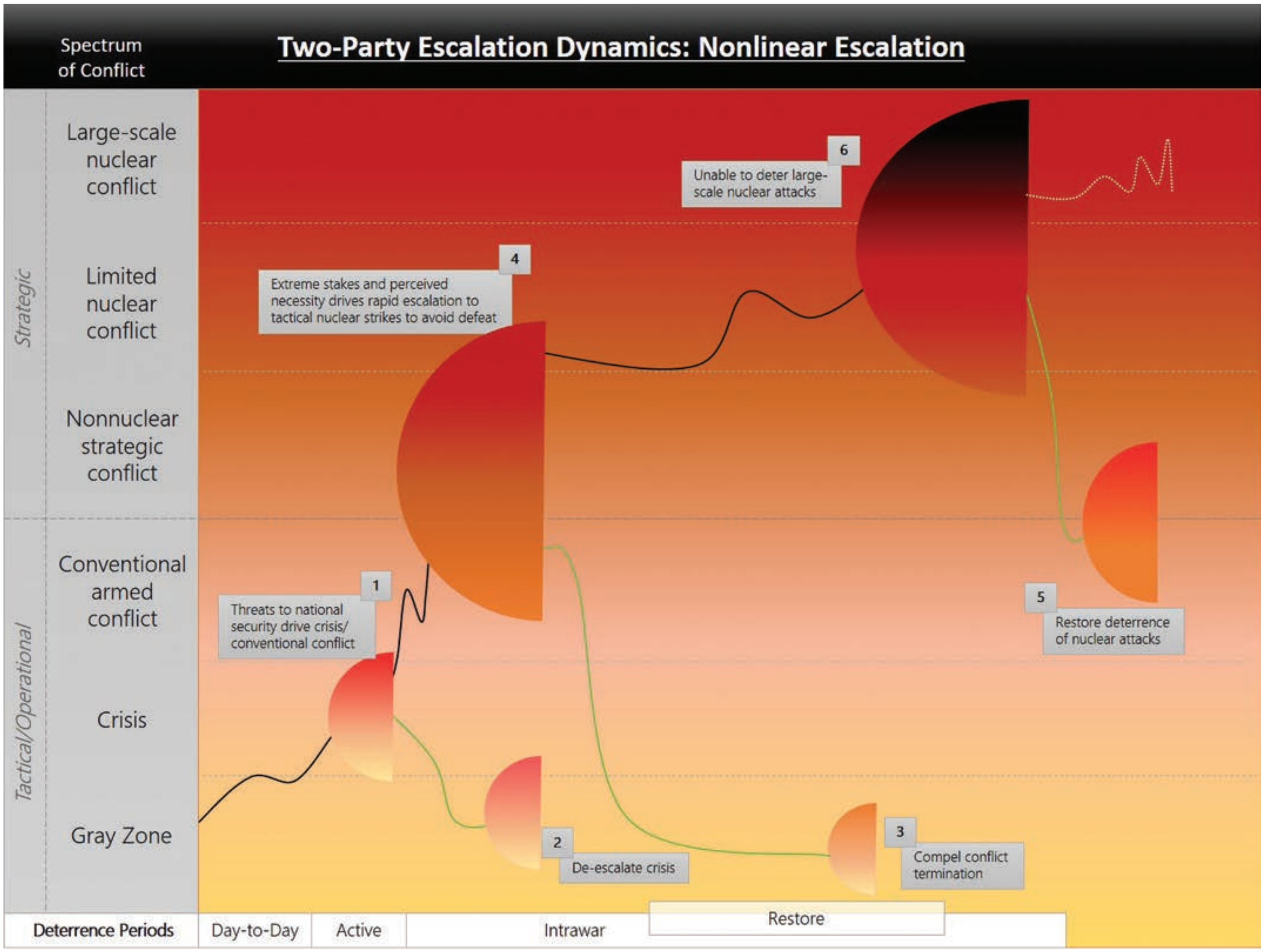
The chaotic nature of escalation dynamics with a strategic adversary may lead to extreme nonlinear escalation rather than the stair-stepping (or ladder-climbing) escalation displayed in figures 1 and 2. The potential for extreme jumps in aggression also depends on things such as the adversary's risk-taking propensity; warfighting strategy and the role of its nuclear weapons therein; force composition and posture; and perceived consequences of defeat and prospects for success. It also depends on the adversary's view of U.S. will and resolve. These factors contribute to the potential of nonlinear escalation, as displayed in figure 3. Here, the adversary perceives rapid escalation to tactical nuclear use as necessary to establish a warfighting advantage and, otherwise, avoid certain defeat (point 3).

An adversary conducting such extreme escalation is a possibility too often dismissed in our war games, plans, and strategies. When it comes to crisis or conflict with a strategic competitor, traditional warfighting strategies that attempt to overwhelm and defeat at the tactical/operational layer with no regard to the strategic layer are dangerously insufficient. As discussed in the next section, the challenge becomes prevailing in the tactical/operational and strategic layers simultaneously.

DBI Periods. Understanding escalation dynamics provides insight into the interplay among varying levels of aggression. As mentioned, key inflection points denote a leader's intentional decision to escalate to a higher level of aggression.[3] These escalation points result in distinct DBI periods: day-to-day, active, intrawar, and restore (see bottom of figures 2 and 3).

Each DBI period prioritizes different objectives and holds its own challenges. As a result, each requires

Figure 3. Nonlinear Escalation


Spectrum of Conflict
Two-Party Escalation Dynamics: Nonlinear Escalation
Large-scale nuclear conflict
Limited nuclear conflict
Nonnuclear strategic conflict
Conventional armed conflict
Crisis
Gray Zone
Strategic
Tactical/Operational
6
Unable to deter large-scale nuclear attacks
4
Extreme stakes and perceived necessity drives rapid escalation to tactical nuclear strikes to avoid defeat
1
Threats to national security drive crisis/conventional conflict
5
Restore deterrence of nuclear attacks
2
De-escalate crisis
3
Compel conflict termination
Deterrence Periods
Day-to-Day
Active
Intrawar
Restore

unique approaches while accounting for the interconnectivity among them. The principal objective of the day-to-day period is to deter aggression and destabilizing behaviors that may lead to a crisis. The challenge of this period is maintaining and upholding deterrence objectives while competing with potential adversaries. Competition strategies seek to advance one's own position relative to another's. Such advantages may include diplomatic relationships and agreements, geographical accesses and territorial claims, military capabilities and capacities, global economic influence, and scientific and technological advancements. In Great Power competition, the ultimate issue at stake is the international order. All these competition objectives run the risk of elevating a competitor's cost of restraint. Thus, day-to-day strategies must manage the tension between competition and deterrence.

The priority objective in the active period is deterring escalation of an existing crisis into full-scale armed conflict. When in a crisis with a strategic competitor, the challenge becomes balancing the need to be decisive with the risk of triggering unnecessary or unintended escalation. Uncertainty of the adversary's intent can risk, on the one hand, indecision or insufficient responses to effectively demonstrate stake and will, resulting in the adversary escalating from a perceived position of strength or advantage (for example, perceived opportunity for a fait accompli). On the other hand, uncertainty of adversary intent can risk overly aggressive actions that drive the adversary to escalate into an unnecessary conflict when, perhaps, the competitor had limited aims to restore or protect national interests that were achievable short of all-out conflict.

Another important consideration for adversary intent is deciphering whether a decision to prosecute conflict has or has not been made. If the adversary has not made the decision, then the primary objective remains deterring armed conflict. If the adversary has made the decision, but has not yet fully carried it out, then the primary objective becomes compellence, or convincing the adversary to change its mind regarding escalation. Recognizing which is called for—deterrence or compellence—is critical to successful influence. Where deterrence approaches are typically more passive, compellence approaches are active. Where deterrence approaches are largely messaging-based, compellence approaches execute previously messaged threats.

In the intrawar period, the primary DBI objective is deterring strategic attack. Depending on the adversary, this could be nuclear, nonnuclear, or both. The intrawar challenge, therefore, is prevailing at both the tactical/operational and strategic levels of war. The tactical/operational level focuses on battlefield advantages on land, on or under the sea, in the air, in space, and in cyberspace. Regardless of domain, the tactical/operational layer is about correlation of forces and capability integration to prevail militarily against the adversary. In doing so, the objective is to compel adversary leadership to de-escalate, but it takes a conventional approach in doing so (that is, strategic influence first requires tactical/operational victory).

The strategic layer focuses on influencing adversary leadership regardless of force correlation. It may include the same military domains, but their application is designed to directly influence the adversary's key decisionmaker(s). In addition, diplomatic, informational, economic, and other tools are used to convince adversary leadership to refrain from escalation or turn the adversary's escalatory behavior around. How to defeat the adversary operationally, while convincing it not to use the means available to escalate out of such defeat, is a wicked problem and the dilemma of the intrawar period.

Finally, the restore period includes two key DBI objectives. The first is to compel termination of ongoing but limited strategic attacks, and the second is to deter large-scale, existentially threatening strategic attacks. The challenge in this period is correcting the failure(s) of previous strategic deterrence attempts in a manner that does not result in further escalation.

If efforts leading to the adversary's strategic attack were insufficient (for instance, inadequate execution) or incorrectly focused (wrong perceptions), how do deterrence planners course correct? The correction cycle may go like this: If an adversary calculated the consequences of its action prior to decision and those consequences were acceptable, then restoring strategic deterrence requires a response that "fixes" those specific perceptions. However, recall the growing uncertainty of such an environment: Determining what those perceptions were, and what they might be now, is extremely difficult. Alternatively, if the adversary's strategic escalation was from a position of necessity (that is, consequences of restraint were unacceptable), then the question at hand is what response (to include self-restraint) might ease those pressures, if one even exists? The worst-case scenario is responding in a way that inadvertently exacerbates consequences of inaction to an extreme that drives large-scale existential escalation.

Interwar Dynamics. As complex as two-party escalation dynamics and DBI periods are, it gets worse when considering the potential for simultaneous crises or conflicts. Multiple priority DBI objectives would exist, and the challenges of an individual DBI period would be complicated by the challenges of others. Moreover, the escalation dynamics of one conflict may interfere with the dynamics of another. An adversary's perceived need or opportunity to escalate may be influenced by the events occurring in another conflict.

Air Force B-52H Stratofortress assigned to 23rd Bomb Squadron prepares to refuel with KC-135 Stratotanker assigned to 91st Expeditionary Air Refueling Squadron in U.S. Central Command area of responsibility during Bomber Task Force mission, March 12, 2023 (U.S. Air Force/Diana M. Cossaboom)

New strategic deterrence frameworks must be tailored not only to distinct potential adversaries but also to the dynamics of specific DBI periods by adversary. In general, approaches for day-to-day DBI are not sufficient for active, intrawar, or restore. We cannot continue the same deterrence activities that were occurring before conflict during conflict, just to a greater extent. Approaches to each DBI period's challenges must be as unique as the challenges themselves. The same applies to whether there is a single crisis or conflict or multiple. If there are multiple, approaches to one must account for the others. In such circumstances, the United States will be pursuing multiple objectives simultaneously, within and across different adversaries, with potentially varying priorities and DBI periods.

Grappling with deterring multiple strategic adversaries under a range of diverse scenarios elevates the importance of understanding interwar dynamics. Interwar deterrence comprises strategies to deter secondary, tertiary, or any additional crises and conflicts from emerging when already engaged in one. It also includes deterring or compelling termination of parallel, duplicative, or opportunistic escalation across multiple ongoing conflicts.

Complexity grows as the number of strategic adversaries increases, their level of coordination deepens, and the range of their escalation options expands. In crises or conflicts, this complexity manifests as a high level of uncertainty regarding potential escalation pathways that the United States must consider and seek to influence. It also increases risks of compounding escalation dynamics. Compounding escalation dynamics may induce higher levels of aggression when multiple strategic adversaries are engaged than would exist when confronting a single competitor.

The extent to which compounding escalation dynamics emerge likely depends on the nature of the relationship between strategic adversaries. Figure 4 exhibits the range of these potential relationships and possible timing of simultaneous crises or conflicts. In general, the risk of compounding escalation dynamics increases as relationships move from misaligned to aligned.

To add another layer of complexity, historical evidence shows these relationships as dynamic. Relations between and among competitors may and would likely evolve according to the level of aggression. What might start as nonaligned and uncoordinated crises may develop into aligned and coordinated, or even allied, simultaneous conflicts. Even if multiple crises or conflicts do not emerge, engagement in one will always include the others as observers with the potential to be more. Thus, strategic deterrence frameworks must account for all strategic adversaries and span across and within varying levels of conflict intensity.

Modern DBI Formula

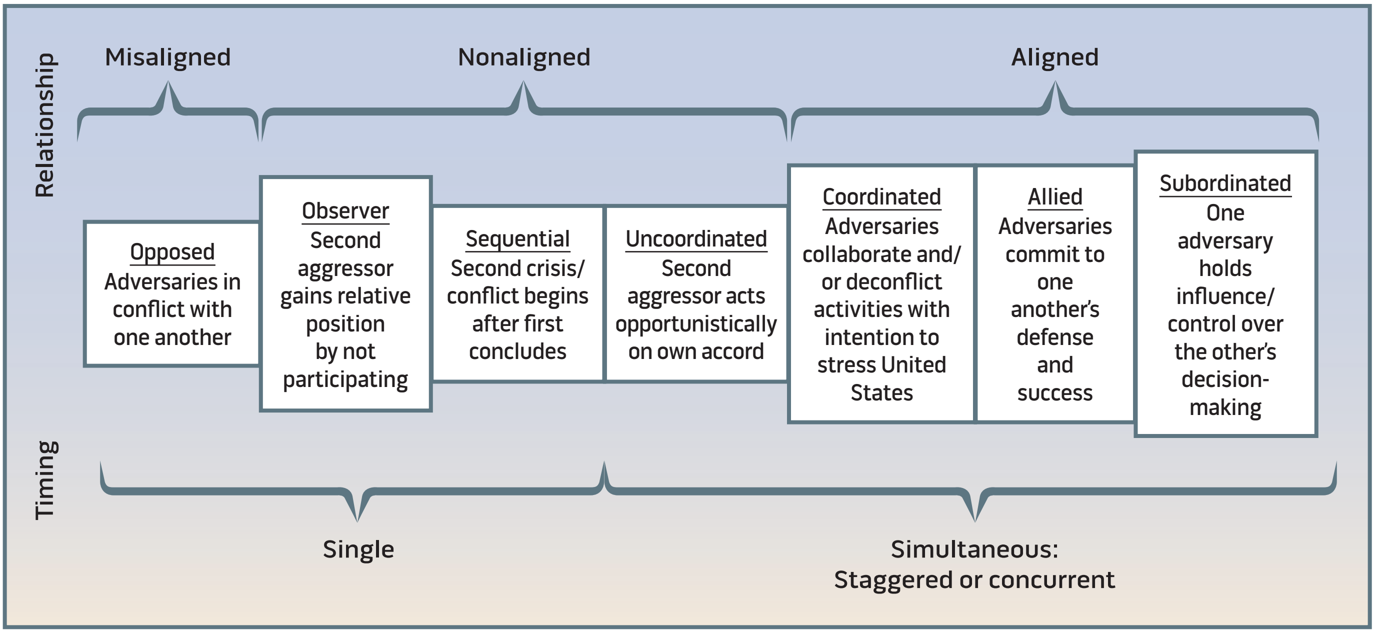
In a multiparty environment, where the United States will be required to pursue multiple DBI objectives simultaneously across varying levels of aggression, the traditional deterrence formula of "deter actor X from action Y in situation Z" is outdated.[4] Rather, a new formula is required that considers multiple potential or ongoing crises or conflicts. A modern DBI formula follows:

Influence actors X_i regarding actions Y_j under Z_k conditions, where

- X_i captures all potential strategic adversaries
- Y_j includes all priority DBI objectives relative to each potential adversary
- Z_k provides context pertaining to the level of aggression for each potential adversary.

Modernized deterrence frameworks keep multiple potential adversaries and multiple DBI objectives in mind.

Figure 4. Spectrum of Relations


Relationship
Misaligned
Nonaligned
Aligned
Opposed
Adversaries in conflict with one another
Observer
Second aggressor gains relative position by not participating
Sequential
Second crisis/ conflict begins after first concludes
Uncoordinated
Second aggressor acts opportunistically on own accord
Coordinated
Adversaries collaborate and/ or deconflict activities with intention to stress United States
Allied
Adversaries commit to one another's defense and success
Subordinated
One adversary holds influence/ control over the other's decision-making
Timing
Single
Simultaneous:
Staggered or concurrent

B-21 Raider is unveiled to public at ceremony on December 2, 2022, in Palmdale, California (U.S. Air Force)

Operations typically designed and/or executed in a particular fashion for a specific actor must now be crafted to achieve a multiadversary effect. This could result in scenarios risking a lower level of effectiveness against the primary adversary for the sake of achieving a greater, multiactor influence. Alternatively, it could result in operations that require a higher level of aggression than would otherwise be necessary but are now appropriate for 2nd or nth party influence. Whereas tailored deterrence strategies traditionally focus on a singular adversary, modern DBI frameworks must have the flexibility and creativity to address multiple adversaries simultaneously.

Conclusion: Necessary Shifts

The unique challenges of today's security environment necessitate an integrated approach to deterrence. Integrated deterrence uses all elements of national power, along with those of U.S. allies and partners, to deter across the spectrum of conflict. Such an integrated approach is critical to influencing all four elements of multiple potential adversaries' decision calculi under a range of circumstances.

Shifting from a singular focus to a multiactor scanner will be the most difficult hurdle to overcome. Shifting requires intellectual diligence and creativity. More fundamentally, it requires fighting the urge to simplify the problem. Too often we narrow our strategy development to fit resource constraints under the way things are typically done. Today's strategists, however, must recognize the threats as they are and face head-on the reality of a complex, congested, and compounding security environment.

Fortunately, there are some best practices that will help. First, let the worst-case scenario become the planning scenario. Specifically, stop restricting analytic curiosity of adversary partnerships and alliances, the scale and scope of such relationships, and the timing of their emergence. A simple review of history's wars shows partnerships and alliances form and separate according to individual actors' security needs. The statement "They would never" should be prohibited from the modern strategist's lexicon.

Second, analyze the interconnectivity of potential adversaries. Understanding an adversary means considering the range of possible paths to escalation with the range of possible conjoining crises or conflicts. In an era of Great Power competition, where the vital national interests of multiple strategic adversaries converge, it is prudent that we connect the dots to see the entire threat landscape.

Finally, increase understanding of potential adversaries' strategic cultures. Understanding a competitor requires understanding its unique history, values, and practices. This should guide strategy development across all DBI periods but may be especially critical for intrawar, restore, and interwar strategies.

A new security environment demands assessing our strategic deterrence approaches to identify the truths that are enduring, the assumptions that no longer hold, and the frameworks that require an overhaul. What was sufficient for previous threat environments is not sufficient today. **JFQ**

Notes

[1] *2022 National Defense Strategy of The United States of America* (Washington, DC: Department of Defense, 2022), https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[2] Another form of compellence, which is not included here, is influencing another to take actions it does not want to take.

[3] While accidents or unauthorized actions may also lead to escalation, these instances fall outside the scope of this article, as their results are unintentional or at least not the intention of the leader whose decision calculus is the target of strategic deterrence frameworks. Nevertheless, these unintentional or unauthorized paths to escalation are necessary to consider and mitigate for a comprehensive security strategy.

[4] *Deterrence Operations Joint Operating Concept, Version 2.0* (Washington, DC: Department of Defense, December 2006), 52, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337.

Two Swedish Air Force Saab JAS 39 Gripens escort U.S. Air Force 23rd Expeditionary Bomb Squadron B-52H Stratofortress over Sweden during Bomber Task Force mission, August 27, 2022 (U.S. Air Force/Michael A. Richmond)

Preventing the Nuclear Jungle
Extended Deterrence, Assurance, and Nonproliferation

By Jennifer Bradley

Today, most people do not remember a time when the United States was not allied with the North Atlantic Treaty Organization (NATO), Australia, Japan, and the Republic of Korea. As these alliances span over seven decades, it is easy to take for granted that the relationships will continue as they always have into the future. In fact, this phenomenon is not as common as it may seem, as only a handful of alliances have had this kind of longevity in the modern era.[1] Based on shared values, common interests, and a shared threat perspective, these alliances have had the safe, effective, and reliable nuclear deterrent of the United States throughout the decades to serve as the cornerstone of the security guarantees provided. The changing security landscape and the emergence of the two-peer nuclear environment will challenge extended deterrence in ways not yet well understood. This requires reexamining deterrence strategies and potentially acquiring new capabilities to effectively assure allies and close the growing "assurance gap."

Dr. Jennifer Bradley is a Senior Deterrence Analyst in the Plans and Policy Directorate at U.S. Strategic Command.

U.S. Policy of Extended Deterrence

The U.S. policy of extended deterrence was born out of the overwhelming conventional threat posed to Western Europe by the Soviet Union at the dawn of the Cold War. To deter Soviet invasion and expansion, the United States extended nuclear deterrence abroad. NATO was created as a nuclear alliance in 1949, with nuclear deterrence made credible by U.S. nuclear forces forward-deployed to NATO serving as the foundation of the collective defense agreement.[2] The policy of extended deterrence was not limited to Europe. In the Pacific, to defend against growing threats from China and North Korea, the U.S. nuclear umbrella expanded to include Australia, Japan, and South Korea, with U.S. nuclear weapons forward-deployed to South Korea, though without NATO-style nuclear-sharing arrangements and fully under U.S. control.

The policy of extended deterrence remains a key component of the security strategy of the United States and its allies. The 2022 Nuclear Posture Review released by the Joseph R. Biden administration affirms the U.S. commitment to extended deterrence, stating that the United States would "[ensure] our strategic deterrent remains safe, secure, and effective, and our extended deterrence commitments remain strong and credible."[3] Furthermore, allies under the nuclear umbrella have reiterated the importance of relying on the U.S. extended nuclear deterrent for their security. The Secretary General's 2022 annual report reaffirmed NATO's status as a nuclear alliance, stating, "As long as nuclear weapons exist, NATO will remain a nuclear alliance."[4]

In 2023, the Washington Declaration affirmed that South Korea "has full confidence in U.S. extended deterrence commitments and recognizes the importance, necessity, and benefit of its enduring reliance on the U.S. nuclear deterrent."[5] Japan's Defense White Paper provides a summary of a U.S.-Japan defense ministerial meeting in which Japan "stated that bilateral efforts at various levels to ensure nuclear deterrence remains credible and resilient [are] more important than ever under the current international security situation."[6] And finally, Australia's National Defence Strategic Review states, "In our current strategic circumstances, the risk of nuclear escalation must be regarded as real. Our best protection against the risk of nuclear escalation is [U.S.] extended nuclear deterrence."[7]

Both the United States and its allies remain committed to extended deterrence, but changes in the security environment mandate a review of the consultative mechanisms and the forces available, as they remain largely unchanged from when they were adjusted after the conclusion of the Cold War. During the Cold War, extended nuclear deterrence was made credible by forward-deploying nuclear weapons into Europe and the Pacific. However, as the security environment changed after the collapse of the Soviet Union, the United States shrank its nuclear footprint, returning most of its nuclear weapons from Europe, and retiring the Tomahawk nuclear sea-launched cruise missile (TLAM-N).[8] While these decisions made sense for the security environment that they were made in, that era has passed. Renewed focus on ensuring the credibility of extended deterrence is necessary to assure allies of their security in a changing security environment.

Challenges to Extended Deterrence

Russia's invasion of Ukraine brought into sharp relief the challenges that the United States and its allies face from revisionist powers dissatisfied with the international system. Threatening nuclear weapons use against both NATO and non-NATO states has become commonplace for Russian officials—a threat made credible by a robust nuclear modernization program focused on improving existing forces and developing novel capabilities.[9] More concerning, the poor performance of Russian conventional forces in Ukraine may lead Russian military strategists to rely more heavily on Russia's expansive tactical and strategic nuclear capabilities to compensate for weakness in its conventional forces.

While the prospects of China's forced unification with Taiwan have dominated security analysis in the last few years, China's ambitions extend much further and include reforming the global governance system to be more in line with its interests. These interests include establishing its own sphere of influence, which places China at odds not only with its regional neighbors concerned about their sovereignty and access to natural resources but also with global nations committed to the rules-based international order.[10] The revelation of Chinese ambitions has been underscored by full-scale conventional and nuclear modernization and expansion. Due to a lack of transparency, China's intentions for its nuclear force remain opaque. However, each year the Department of Defense's report, the *Military and Security Developments Involving the People's Republic of China*, increases its estimate of the future size of China's nuclear arsenal, with the 2022 report stating China could possess a nuclear stockpile of 1,500 weapons by 2035.[11] The rapid growth of China's nuclear arsenal allows it to adapt its nuclear strategy in any way it deems necessary to address its security concerns and achieve its strategic objectives.

When comparing the challenges posed by Russia and China to those of North Korea, it is tempting to diminish the threat because it is not to the same scale. But that could be a mistake. Continued advancements in North Korean missile technology and growth of its nuclear force means that it poses a credible threat to the homelands of the United States and our Indo-Pacific allies.[12] Moreover, North Korea's nuclear doctrine calls for "preemptive and offensive nuclear strike," with credible nuclear forces capable of preemptive attack and nuclear warfighting.[13] Coupled with North Korea's history of provocation, the potential for miscalculation on the Korean Peninsula continues to increase.

While it is customary to examine each threat separately, the threats become more acute when examined together. Furthermore, strategists must consider

Maintainers assigned to 393rd Expeditionary Bomb Squadron prepare B-2 Spirit for its first hot pit refueling at Ørland flystasjon, Brekstad, Norway, August 29, 2023 (U.S. Air Force/Heather Salazar)

the potential for these adversaries to work in unison to achieve their aspirations, especially given that each adversary has identified the United States and its allies as security threats and an impediment to achieving its national security objectives. Prior to Russia's invasion of Ukraine, China and Russia released a communiqué describing their relationship as a no-limits friendship. While the latest communiqué reframed the relationship as a "comprehensive partnership," what is clear is that cooperation between these two states will continue and grow for the foreseeable future.[14] While North Korea's relationship with China and Russia has often been volatile, with North Korea always careful not to become overly reliant on—and therefore vulnerable to—both nations, recently it has increased its overtures of cooperation to build strategic partnerships with both China and Russia.[15] The prospect of cooperation and potentially collaboration between or among these nations will challenge extended deterrence in the next decades.

The Assurance Challenge

The terms *extended deterrence* and *assurance* are often used interchangeably, but while the concepts are related, they are focused on different audiences. Extended deterrence is directed at influencing adversaries to prevent attacks on allies, while assurance is directed at convincing allies of U.S. commitment to their defense. Just as deterrence is a cognitive function in the mind of the adversary, assurance is a cognitive function in the mind of the ally. Both rely on perceptions of the capability, credibility, and will of the United States to defend its vital interests and meet its security obligations.

Assuring allies is inherently difficult. While Thomas Schelling's Nobel Prize–winning research on deterrence described the benefits of uncertainty or "the threat that leaves something to chance" for deterrence, assurance of allies requires a greater level of certainty and credibility because allies are unwilling to leave their security to chance.[16] Nor should they be expected to. This challenge has been deliberated for decades, with analysts and policymakers debating the question, "Would the United States sacrifice San Francisco for Tokyo or Boston for Prague?" It is a question that generates tremendous anxiety for the allies under the nuclear umbrella because their security depends on the answer.

This anxiety is made substantially worse because the most likely pathways for potential nuclear use begin with regional conventional conflict escalating to limited nuclear use, meaning that our allies are on the frontlines for this threat. Compounding this anxiety are the investments both Russia and China have made into low-yield theater nuclear weapons. These weapons can hold the allies at risk and grow North Korea's nuclear arsenal while potentially lowering the threshold for use. Furthermore, deterring opportunistic aggression in one theater while the United States is fully engaged in another will challenge extended deterrence, heightening allies' anxiety and decreasing their confidence in extended deterrence meeting their security needs.

Risk to the Nonproliferation Agenda

The 2022 National Defense Strategy reiterates the U.S. commitment to nonproliferation of nuclear weapons, a commitment the United States has held since the mid-20th century. A key driver for providing a nuclear umbrella for allies was to reduce the necessity for them to develop their own nuclear capabilities to meet their security needs. This allowed allies to forgo their nuclear ambitions and accede to the Nuclear Non-Proliferation Treaty as nonnuclear states, strengthening the nonprolifera-

tion regime. In fact, the Department of State has stated, "Nuclear umbrella security agreements, whether unilateral or multilateral, have been, and are expected to continue to be, effective deterrents to proliferation."[17] The risk if allies under the nuclear umbrella lose confidence in extended deterrence, determining that their security needs are no longer met by U.S. guarantees, could potentially put pressure on allies to develop their own nuclear weapons, undermining the nonproliferation regime.

Recently, this risk has become more acute. President Yoon Suk Yeol of South Korea suggested in 2023 that the Republic of Korea may have to consider building its own nuclear weapons to confront its deteriorating security environment. These suggestions came after the announcement that South Korea will stand up its own Strategic Command in 2024 charged with the mission of addressing the North Korean nuclear threat and commanding the South's strategic forces, to include conventional ballistic missiles, missile defenses, and space and cyber capabilities, to name a few.[18] These moves have been popular with the public, with polling suggesting the South Korean public overwhelmingly supports the country's acquiring its own nuclear deterrent.[19]

While South Korea has the most public support for developing a nuclear capability, it is not the only nation under the nuclear umbrella contemplating such a move. The governments of both Japan and Australia, traditionally staunchly against building a nuclear capability of their own, have more openly discussed the merits of, at a minimum, nuclear-sharing agreements. Some in the Japanese government have been more forward leaning. Former Japanese Defense Minister Shigeru Ishiba stated in 2017, "Japan should have the technology to build a nuclear weapon if it wants to do so."[20] Moreover, it must be noted that these nations are more than technically capable of developing nuclear weapons and it is political considerations that have served as a restraint. As those political considerations continue to change, they may no longer serve as a restraint but as a catalyst for proliferation.

Mitigating the Risk to Assurance

Assuring our allies is an imperative, not only for the health of the nonproliferation regime but also for the continued strength of the alliance relationships. The benefits that the United States receives from strong alliances are numerous. These relationships contribute to global stability and prosperity by binding powerful nations together with a shared vision and purpose. Also, by building militaries that are interoperable and exercising in peacetime, these alliance relationships increase the involved nations' overall military strength, thus enhancing deterrence. Failing to mitigate the risk to assurance could introduce stress into the alliances, undermining cooperation and creating the potential for global instability with the increased risk of arms races and growing competition.

To address the challenge, the United States must remain committed to the nuclear modernization program. The potential for productive relationships with Russia and China, the focus on the war on terror, and continued conflicts in the Middle East resulted in decisions for nuclear modernization being delayed. While the programs are under way, they are at a point that any delay in funding or technical issues may result in an increase in risk.

While it is imperative that the modernization program stays on track, the decisions for the program were made in 2010, in a more benign security environment. Since that time, the increased aggression of Russia, the strategic breakout of China, and the continued

Ohio-class ballistic-missile submarine USS *Kentucky* arrives for port visit in Busan, Republic of Korea, July 18, 2023 (Screenshot/U.S. Navy Video/Adam Craft)

advancement of North Korea's nuclear program require the United States and allies to reevaluate their strategy to confront these new security threats. NATO has begun that process with the Vilnius Summit Communiqué, announcing a new generation of strategic plans to increase readiness and improve deterrence of threats.[21] However, any new strategy must address the risk to extended deterrence of the two-peer environment and the risk of opportunistic aggression from one adversary if the United States is engaged with the other. Therefore, any strategy for Europe must consider the risk of opportunistic aggression in the Indo-Pacific region and vice versa. This will place additional demands on both the allies and the United States to ensure an effective deterrent.

Although it is tempting to immediately discuss the capabilities needed for extended deterrence and assurance, ensuring that the strategy is sound is a necessary first step. This leads to a more fruitful debate on what capabilities are needed to make the strategy credible. While each leg of the triad is being replaced, a mix of both conventional and nuclear capabilities is necessary to meet both the military and political requirements for extended deterrence. Militarily, the forces must be survivable and prompt while also capable of holding a variety of adversary targets at risk. Strategically, the forces must provide a persistent presence, be visible to the adversary, while also being acceptable to the ally and potentially providing the option for burden-sharing.[22] Through consultations, the United States and allies should develop a suite of capabilities to make the extended deterrence strategies credible. Working directly with allies will also enhance assurance.

Consulting with allies is imperative for assurance, and to that end, the United States is modernizing and enhancing the processes for consultations within the alliances. Today, these processes are quite different between the Indo-Pacific allies and the NATO allies. There may be benefits in creating NATO-like consultative mechanisms and processes for the Indo-Pacific allies. This would increase assurance by ensuring allies feel that they are actively involved in decisions affecting their security. Additionally, building mechanisms to conduct combined deterrence planning across deterrence periods and spectrums of conflict will better allow the alliances to integrate deterrence operations. The Washington Declaration has laid the foundation for building these mechanisms with South Korea, announcing the establishment of a Nuclear Consultative Group charged with increasing nuclear dialogue, information-sharing, and strategic planning.[23] Finally, the security environment necessitates that NATO allies and Indo-Pacific allies work together to address security threats. Strengthening relationships across regions and nations will enhance deterrence throughout an increasingly interconnected security environment.

Conclusion

The grand bargain of extended deterrence is a unique aspect of U.S. alliance relationships. Elaine Bunn, the former Deputy Assistant Secretary for Nuclear and Missile Defense Policy, testified before Congress on this phenomenon, remarking:

> *I have come to believe that extended deterrence is amazing from both sides. We have our non-nuclear allies, who have forsworn*

> *their own nuclear weapons and rely on another country, the U.S., in high-end situations, including nuclear attacks on their own territory and people. And it is amazing that the U.S. takes on the risk and responsibility of putting its own forces, even its population and territory, at risk on behalf of an ally. And that is an amazing fact to the point that some, in the past, have found it incredible.*[24]

The emerging two-peer environment will increasingly challenge this "amazing" agreement.

The credibility of extended deterrence is being directly tested by our potential adversaries as they pursue their goals that increasingly challenge the security of the United States and its allies. The consequences of failing to assure allies could dramatically change the international environment. Failing to address the challenges to assurance increases the risk of nuclear proliferation by allies. General Cotton testified to this risk, stating, "The credibility of our extended deterrence commitments is not only part of the nation's ironclad commitment to our allies, but it's also essential in limiting proliferation of nuclear weapons."[25] Mitigating this risk requires reexamining our strategies, designing an extended deterrence posture with both conventional and nuclear weapons to achieve that strategy while modernizing the alliance structures and consultative mechanisms that increase alliance integration. This requires the United States to be open and increase consultations, especially with our East Asian allies, on nuclear deterrence strategies and their respective employment.

Every conflict the United States has fought since World War I has involved allies. They are the greatest asset of the United States, and it is easy to take the U.S. alliance system for granted because of the longevity of the relationships. However, in the next decades, the challenges to extended deterrence and assurance will only increase. The United States needs to take proactive action now to enhance extended deterrence and mitigate the risk to assurance to ensure our allies that the U.S. commitment is "ironclad." Failing to close the gap might have consequences that could dramatically reshape the security environment. During World War II, Winston Churchill observed, "There is only one thing worse than fighting with allies and that is fighting without them."[26] By placing alliances on a solid footing for decades to come, prioritizing extended deterrence and assurance will ensure that the United States does not face Churchill's worst-case scenario. **JFQ**

Notes

[1] Patrick T. Warren, *Alliance History and the Future NATO: What the Last 500 Years of Alliance Behavior Tell Us About NATO's Path Forward* (Washington, DC: Brookings Institution, June 30, 2010), 51–56, https://www.brookings.edu/wp-content/uploads/2016/06/0630_nato_alliance_warren.pdf.

[2] "NATO's Nuclear Deterrence Policy and Force," NATO, July 5, 2023, https://www.nato.int/cps/en/natohq/topics_50068.htm.

[3] *2022 Nuclear Posture Review* (Washington, DC: Department of Defense, 2022), 7, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF#page=33.

[4] *The Secretary General's Annual Report 2022* (Brussels: NATO, 2022), 25, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/sgar22-en.pdf#page=27.

[5] The White House, *The Washington Declaration*, April 26, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/washington-declaration-2/.

[6] *Defense of Japan 2023* (Tokyo: Ministry of Defense, 2023), 365.

[7] *National Defence: Defence Strategic Review 2023* (Canberra: Australian Government, 2023), 38.

[8] *China's Emergence as a Second Nuclear Peer: Implications for U.S. Nuclear Deterrence Strategy* (Livermore, CA: Center for Global Security Research Study Group at Lawrence Livermore National Laboratory, 2023), 47.

[9] Michaela Dodge, *Alliance Politics in a Multipolar World* (Fairfax, VA: National Institute Press, October 2022), 13–18.

[10] Jennifer Bradley, *China's Nuclear Modernization and Expansion: Ways Beijing Could Adapt Its Nuclear Policy* (Fairfax, VA: National Institute Press, July 2022), 11–16.

[11] *Military and Security Developments Involving the People's Republic of China 2022: Annual Report to Congress* (Washington, DC: Office of the Secretary of Defense, 2022), ix.

[12] *2022 Nuclear Posture Review*, 5.

[13] Bruce Klingner, *The Troubling New Changes to North Korea's Nuclear Doctrine*, Backgrounder no. 3729 (Washington, DC: The Heritage Foundation, October 17, 2022), https://www.heritage.org/asia/report/the-troubling-new-changes-north-koreas-nuclear-doctrine.

[14] Stefan Wolff, "The Russia-China Relationship: The Perils of a 'Friendship With No Limits,'" *UK in a Changing Europe*, April 5, 2023, https://ukandeu.ac.uk/the-russia-china-relationship-the-perils-of-a-friendship-with-no-limits/.

[15] Mike Chinoy, "Kim Jong Un Is Putin's and Xi's New Best Friend," *Foreign Policy*, September 12, 2022, https://foreignpolicy.com/2022/09/12/north-korea-russia-china-partnership-putin-xi-kim/.

[16] See Thomas C. Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960).

[17] David J. Trachtenberg, "U.S. Extended Deterrence: How Much Strategic Force Is Too Little?" *Strategic Studies Quarterly* 6, no. 2 (Summer 2012), 67.

[18] Daehan Lee, "South Korea to Create New Command That Would Control Strategic Weapons," *Defense News*, July 11, 2022, https://www.defensenews.com/global/asia-pacific/2022/07/11/south-korea-to-create-new-command-that-would-control-strategic-weapons/.

[19] Katrin Fraser Katz, Christopher Johnstone, and Victor Cha, "America Needs to Reassure Japan and South Korea," *Foreign Affairs*, February 9, 2023, https://www.foreignaffairs.com/japan/america-needs-reassure-japan-and-south-korea.

[20] "Japan Should Be Able to Build Nuclear Weapons: Ex-LDP Secretary General Ishiba," *The Japan Times*, November 6, 2017, https://www.japantimes.co.jp/news/2017/11/06/national/japan-able-build-nuclear-weapons-ex-ldp-secretary-general-ishiba/.

[21] *Vilnius Summit Communiqué*, NATO, July 11, 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

[22] *China's Emergence as a Second Nuclear Peer*, 49.

[23] The White House, *The Washington Declaration*, 2023.

[24] Statement of M. Elaine Bunn, *Hearing to Receive Testimony on Regional Nuclear Deterrence*, Senate Armed Services Committee, 118th Cong., 1st sess., March 28, 2023, Washington, DC, https://www.armed-services.senate.gov/imo/media/doc/23-21_03-28-2023.pdf.

[25] Cotton, "SASC Fiscal Year 2024 U.S. Strategic Command and U.S. Space Command Posture Hearing."

[26] "D-Day: FDR and Churchill's 'Mighty Endeavor'," n.d., Franklin D. Roosevelt Presidential Library and Museum, Hyde Park, NY, https://www.fdrlibrary.org/mighty-endeavor.

Unarmed Air Force Minuteman III intercontinental ballistic missile launches during operational test, May 3, 2017, at Vandenberg Air Force Base, California (U.S. Air Force/Daniel Brosam)

Don’t Get Lost in the Numbers

An Analytic Framework for Nuclear Force Requirements Debates

By Patrick McKenna and Dylan Land

Patrick McKenna is Senior Technical Advisor in the Plans and Policy Directorate at U.S. Strategic Command (USSTRATCOM). Dylan Land is a Deterrence Analyst Contractor assigned to the Plans and Policy Directorate at USSTRATCOM.

The international strategic landscape is rapidly evolving. Shifting balances of power, galloping technological change, and emboldened opposition to the rules-based international order pose discrete challenges to U.S. national security and that of its allies and partners. The most consequential shift may be the pace with which the People’s Republic of China

(PRC), the Russian Federation, and the Democratic People's Republic of Korea (DPRK or North Korea) are expanding and diversifying their strategic capabilities, each increasing its reliance on nuclear weapons to achieve national objectives. When viewed in their totality, such changes constitute a generational challenge for which the United States must develop a prevailing national strategy.

Nuclear weapons and their unique deterrent effects have long been the cornerstone of U.S. national security and a steadfast pillar of international stability. The United States has, for decades, sought to maintain a safe, secure, and effective nuclear force.[1] As U.S. competitors, principally China and Russia, modernize their nuclear weapons complexes and field advanced nonnuclear strategic capabilities, U.S. leaders recognize that "deterrence now demands far more coordination, innovation, and cooperation from us all."[2] In such an environment, the United States must continue reassessing the role and effectiveness of nuclear forces in safeguarding America's vital interests—in part by implementing "integrated deterrence" as outlined in the U.S. National Defense Strategy.[3]

Some analysts may observe China, Russia, and North Korea augmenting their nuclear arsenals and missile capabilities and justifiably conclude that the United States needs to increase the size of its own nuclear stockpile. While the balance of nuclear forces is a key input into deterrence calculations, emergent geostrategic risks are not just nuclear. Strategic deterrence involves confidence in being able to cover targets and execute deliberate nuclear plans, but a larger set of considerations necessarily affect the probability of U.S. deterrence success or failure. A prescient and responsive U.S. strategy cannot focus solely on the quantity of nuclear weapons because some potential threats cannot be credibly deterred by simply having more nuclear weapons. To be clear, debates surrounding nuclear force sizing are necessary—but nuclear weapons alone may not solve 21st-century deterrence challenges.[4]

This article proposes an approach to nuclear force sizing debates based on a framework built on four analytic dimensions: overarching risk management approaches; deterrence and assurance objectives; strategic force employment guidance; and operational constraints. The answers to key questions across these dimensions provide a structure to inform debates about the appropriate size and characteristics of U.S. nuclear forces. Only after clarifying U.S. objectives across these dimensions and focusing on key considerations therein should policymakers enter nuclear force sizing debates. The resulting analysis does not advocate for any policy position or hypothesize the "correct" number of nuclear forces. Instead, the purpose of the framework is to focus nuclear force sizing debates on more fundamental assumptions regarding the role of nuclear weapons in achieving U.S. national security objectives.

Strategic Environment

The PRC, under the leadership of General Secretary Xi Jinping, is accelerating its military modernization programs, with many anticipating dramatic changes to Beijing's nuclear force composition.[5] The U.S. Department of Defense (DOD) estimates that "the PRC's operational nuclear warheads stockpile has surpassed 400" and "will likely field a stockpile of about 1,500 warheads by its 2035 timeline," if current trends continue.[6] Meanwhile, Russia is completing a decades-long nuclear modernization program and continuing to invest in a growing arsenal of more than non-treaty-accountable (colloquially referred to as nonstrategic, or tactical) nuclear weapons.[7] The DPRK has also made "significant advances over the past two decades in developing a nuclear weapons arsenal," with some estimating that Pyongyang has sufficient fissile material to build 45 to 55 nuclear weapons, with 20 to 30 potentially assembled.[8]

The PRC, Russia, and the DPRK are also raising the salience of nuclear weapons in their military strategies "to secure coercive and military advantage against the United States, and its allies, and partners."[9] Beijing has engaged in assertive behavior in the Taiwan Strait and the Indo-Pacific region, Russia's Vladimir Putin has heightened nuclear risks in his attempts to dissuade continued Western support for Ukraine, and Kim Jong Un oversaw the passing of a new law that expands the conditions under which North Korea would use nuclear weapons.[10]

Numbers Debates

Some analysts contend that if the most consequential potential U.S. adversaries are developing more nuclear weapons, so should the United States. Such arguments are not without basis. The 2010 New START Treaty limits U.S. nuclear forces to 1,550 deployed strategic nuclear weapons and 800 deployed and nondeployed delivery vehicles. The world has changed significantly in the past 14 years, and the risks to deterrence have unambiguously grown. Others may look to the Treaty on the Prohibition of Nuclear Weapons—which currently has 92 signatories—and Russia's nuclear intimations in Ukraine to argue that the world needs to *decrease* the number of deployed nuclear weapons.

Numbers of nuclear weapons can inform and shape strategy, but no matter the frame of reference, seeking more or fewer nuclear weapons is not a strategy in and of itself. It is a desired endstate. If every challenge could be overcome through strategic nuclear deterrence, a simple answer of adding more nuclear weapons to the deployed U.S. stockpile would be an obvious solution. But there are many risks that nuclear weapons alone cannot overcome and many considerations that go into determining which force postures and employment guidelines are achievable. This is not to argue that other capabilities, either military or nonmilitary, can replace the unique deterrent effects of nuclear weapons. Rather, as U.S. national guidance has focused leaders on a strategy of integrated deterrence, it is imperative to understand where and how other capabilities can support the U.S. nuclear enterprise in deterring strategic attacks against the United States, its allies, and its partners.

Debating the merits of different nuclear force sizes without clear reflection back to underlying U.S. strategic objectives puts the cart before the horse. Nuclear force sizing debates can distract from much more important discussions about underlying assumptions and beliefs about the role of nuclear weapons in U.S. national security.

Before advocating for nuclear force sizes, analysts should identify the attributes and characteristics of nuclear weapons most relevant to achieving U.S. objectives set by broader national security strategies. The appropriate composition of U.S. nuclear forces must factor in considerations across dimensions of risk management; deterrence and assurance objectives; strategic force employment; and operational constraints. By analysts' following an analytical method, the necessary attributes and characteristics of nuclear forces should become clearer. Such an approach drives strategy debates and not just force sizing debates.

Proposed Framework

The following section proposes a framework to refocus U.S. nuclear policy and strategy debates on key questions across interdependent and interrelated analytic dimensions: risk management; deterrence and assurance objectives; strategic force employment; and operational requirements. *Risk management* refers to the overarching strategy for navigating geopolitical, technological, programmatic, and operational risks. *Deterrence and assurance objectives* help determine the capabilities necessary to prevent strategic attack on the United States and its allies and partners. Based on the profile of risk and the identified objectives, policymakers outline *strategic force employment* guidance for a given challenge. Such guidance and analysis must consider the *operational requirements* of maintaining a particular posture or executing certain plans. Key considerations within each dimension guide discussions to the heart of many assumptions about the required size of the U.S. nuclear arsenal by isolating where and how nuclear weapons are most useful in achieving national security objectives—and where they are not.

The questions outlined below may not—and in some cases should not—be precisely answered in public forums. Policymakers prefer to build in ample decision space for leaders, particularly where nuclear weapons are concerned, and explicit answers to the questions in each dimension could constrain that decision space. If, for example, the United States outlined exactly what it sought to deter, potential adversaries may perceive false comfort in misbehaving under those deterrence thresholds, which could impinge on other national interests.

Risk Management Considerations

Risk management has been a key component of U.S. national strategy and nuclear force sizing debates for more than 30 years. Reframing policy and strategy choices as an exercise in risk management emphasizes the trade space between different possible solutions and requires policymakers to evaluate a broader set of capabilities in pursuit of that solution. Risk management requires leveraging U.S. capabilities across the interagency community and among international allies and partners—one of the primary objectives of integrated deterrence. For example, shaping potential adversaries' perceptions is a key objective of deterrence. If the objective is framed as a nuclear policy choice, proposed solutions may help to adjust the number of deployed nuclear weapons. If, however, the challenge is posed as one of risk management, there is more space to evaluate other means of influence (for example, diplomacy, economic punishments, or incentives). Both approaches may yet result in a similar recommendation, but intentionally framing objectives through a broader risk management lens requires analysts to examine how nuclear weapons fit among other U.S. instruments of power.

The proposed framework focuses on four categories of risk: geopolitical, technological, programmatic, and operational.[11] China's nuclear expansion is an example of a realized geopolitical risk. Technological risks include those that could undermine the effectiveness of U.S. nuclear weapons systems, such as breakthroughs in advanced missile defenses. Programmatic risks refer to potential delays in U.S. nuclear modernization programs. Operational risks encompass delays to force generation, force availability constraints, unanticipated changes to operational requirements, and so forth. Each category of risk has implications for determining the appropriate attributes and characteristics of U.S. nuclear forces.

Geopolitical Risk. Different actors' behaviors shape geopolitical trends and in turn condition the nature of states' interactions, the profile of developing risks, and balances of power around the world—depending on the relative successes or failures of a particular country's goals. Given this, geopolitics shape the strategic landscape and inherently underwrite all dimensions of policy and strategy analysis as well as other risk factors. Emergent risks and potential threats that warrant a deterrence policy derive from the geopolitical environment. The security landscape shapes allies and partners' risk assessments as well the perceived credibility of U.S. commitments. The objectives guiding targeting and strategic force employment guidance are derived from geopolitics. Operational considerations necessarily reflect the geopolitical landscape because it is the environment in which operations must be conducted today and planned to be executed in the future. Key questions include:

- What risks to U.S. national security may materialize from geopolitical change?
- To which of these risks can nuclear weapons policy and strategy be credibly applied?
- For which risks are nuclear weapons insufficient?

By answering these questions, analysts may begin to identify the attributes of a nuclear force necessary to achieve U.S. national security objectives. The last question in particular helps identify areas in which other instruments of power may be more useful than nuclear weapons alone in achieving U.S. objectives.

Air Force B-2 Spirit assigned to 509th Bomb Wing taxis at Joint Base Elmendorf-Richardson, Alaska, July 19, 2023, as part of bomber Agile Combat Employment exercise (U.S. Air Force/Julia Lebens)

Technological Risk. Disruptive technologies have the potential to alter geopolitics in unpredictable ways. Applying advanced technologies—such as artificial intelligence, quantum computing, autonomous vehicles, and entangled digital platforms, among others—to military operations challenges core assumptions about escalation dynamics and system vulnerability. Successive U.S. administrations have sought to capture the cross-domain deterrence challenges of technological change within their national defense strategies, "integrated deterrence" being the latest manifestation. A growing portfolio of novel delivery systems also has important implications for deterring strategic attacks. Such innovations could further complicate an already precarious geopolitical balance by influencing conflict dynamics, gray zone escalation, systems reliability, and war planning. Deploying a nuclear force that can adapt to such technological change should be a key objective for U.S. policy and strategy. Key questions include:

- What present and future technological trends pose the greatest risks to U.S. national security?
- What role can nuclear weapons have in mitigating such risks? How might changes to U.S. nuclear forces (either in number or posture) affect technological risks?
- What technological risks is the United States willing to accept?

Programmatic Risk. The most important considerations of programmatic risk for nuclear force sizing are those concerning the time schedule for new systems coming online. The United States remains committed to fielding a triad of strategic nuclear capabilities composed of a sea leg (ballistic missile submarines), an air leg (weapons delivered via B-2 and B-52 strategic bombers), and a ground force of intercontinental ballistic missiles (Minuteman III), complemented by forward-deployable dual-capable aircraft (DCA). The nuclear modernization program covers all three legs of the nuclear triad and DCA capabilities; their supporting nuclear command, control, and communications network; and the underlying industrial base required to meet production demands. Nevertheless, modernization and recapitalization efforts do influence the flexibility of U.S. nuclear forces and the capacity to field more or fewer at any given time. The answers to the following questions highlight ways in which programmatic risks could affect the desired size and posture of U.S. nuclear weapons. Key questions include:

- How might delays in nuclear modernization and recapitalization programs affect currently fielded forces?
- Would adjustments to force size and posture mitigate some of those risks? If so, to what end?

U.S. Air Force 23rd Bomb Squadron B-52H Stratofortress, two German air force Panavia Tornados followed by two German air force Eurofighter Typhoons, and one Belgian air force F-16 Fighting Falcon fly in formation over Germany during Bomber Task Force mission, August 24, 2022 (U.S. Air Force/Michael A. Richmond)

- What are other risks associated with the transition to replacement weapons systems?

Operational Risks. Any change in nuclear policy has implications for operational requirements. These operational considerations (for example, how many personnel are needed for a certain posture) are explored below. Changes to policy and strategy in peacetime or in early stages of crisis necessarily affect force availability and flexibility during times of increasing tensions or conflict. There is a risk of resource (mis)allocation because of deliberate force structure decisions that could affect nuclear operations. It is therefore important to explore the operational risks associated with changes in nuclear policy long before analysts advocate for such changes. Key questions include:

- What redundancies or reinforcing attributes are necessary in the force to minimize, or distribute the burden of, operational risks?
- How do other mission sets (for example, conventional theater war) affect availability of capabilities to support nuclear operations?
- How does the possibility of unanticipated operational risks affect the necessary characteristics and attributes of the U.S. nuclear force?

Deterrence and Assurance Considerations

Deterrence. Deterring strategic attack remains the cornerstone of U.S. national security. Even in the most benign security environment, the United States would seek to deter strategic attacks against itself and its allies and partners. Not every potential threat, though, is grave enough to justify an explicit U.S. deterrence policy;

deterrence is inherently costly. There are risks associated with carrying out a threatened (or implied) response if deterrence fails. Punishment is not, however, the only means of deterrence. The United States can deter certain behaviors if it can convince the potential actor that it will be denied the benefits of acting in the first place, but that involves investing in means to deny those benefits. Regardless of the means of deterrence, the United States must have sufficient stake in the consequences of a particular behavior to be willing to inherit the risks associated with responding or make the necessary investments to deny successful manifestation of the behavior in the first place. Determining which risks the United States would have the capability and will to deter is a key component of identifying the desired characteristics and attributes of nuclear forces. Key questions include:

- What actions does the United States seek to deter?
- Which of those actions can nuclear weapons credibly and effectively deter?
- To which potential threats is the application of nuclear deterrence insufficient or noncredible?
- Where and how might a potential adversary perceive a plausible advantage of "breaking" U.S. deterrence?
- Are there certain periods (for example, peacetime, intrawar) where deterrence failure is more likely?

Assurance. Assurance is not only about military capabilities; it also relies as much on policy and strategy. During the early Cold War, for example, U.S. policy relied on threats to initiate general nuclear war against the Soviet Union if Moscow invaded West Germany.[12] While the United States certainly had the capabilities to execute such a mission and the Soviet Union ultimately did not invade West Germany, some U.S. allies questioned "American firmness" on its extended deterrence policy.[13]

Assurance comprises efforts to convince allies and partners that the United States has the capability and will to incur the risks of deterring attacks on their countries. Allies and partners may be more assured if they believe their national security is a U.S. vital interest and that the United States can deter efforts to undermine that interest. Assurance considerations are thus intrinsically bound to core U.S. deterrence objectives. If the United States, its allies and partners, and a potential adversary all perceive U.S. strategy as credible, both deterrence and assurance objectives are satisfied. However, deterrence alone does not suffice for assurance. If only the United States and a potential adversary perceive a U.S. strategy as credible, assurance objectives may not be met even if deterrence is successful. Key questions include:

- Does assurance require nuclear force adjustments beyond those required for deterrence?
- Are allies convinced that potential adversaries perceive U.S. extended deterrence commitments as credible? If not, why not?

Strategic Force Employment

Nuclear weapons force employment guidance is signed by the U.S. President and further refined by the U.S. Secretary of Defense and Joint Chiefs of Staff.[14] Planners then "develop specific military objectives . . . that are designed collectively to achieve specified endstates."[15] Once identified, objectives guide planners as they develop options to achieve them.[16] Analysts advocating for particular nuclear force sizes must first account for these force employment considerations because "U.S. strategy for nuclear employment informs its force sizing and posture decisions."[17]

Simply put, strategic force employment guidance is driven by strategic and military objectives. Any nuclear force should maintain the capability to achieve those objectives to include directed flexibility in achieving them. Guidance directs some flexibility (that is, providing multiple options to the President), and the force composition enables flexibility (even in cases when it is not directed). Such flexibility can change over time, either due to direction, changes in force composition, or adversary action. Yet nuclear weapons are part of a broader array of strategic capabilities, and therefore other tools may be able to support nuclear force employment in achieving a desired objective. For example, improvements in nonnuclear weapons systems may decrease the number of nuclear weapons necessary to satisfy a particular objective. Whether or not some of these conventional capabilities can be reserved for executing strategic objectives has implications for nuclear force sizing.

Strategic force employment considerations for nuclear force sizing require that analysts focus on objectives identified by higher leadership, evaluate the attributes and characteristics necessary to achieve those objectives, and assess how other capabilities can support such missions. Key questions include:

- How does the United States prioritize different political and military objectives with the nuclear force?
- How much flexibility (that is, ability to achieve objectives under different conditions and in different ways) is desired in the U.S. nuclear force?
- To what extent can the employment burden be mediated by nonnuclear capacities (that is, are nonnuclear capabilities considered a replacement for or augmentation to nuclear capabilities)?
- What objectives does the United States need to be able to achieve against countries simultaneously (if any)?
- What forces would be required to immediately address escalation?
- What forces would be required to maintain/restore deterrence thereafter?
- What objectives does the President want to achieve?
- What adversaries does the President direct planning against?

Operations

Any desired nuclear posture requires additional forces beyond those deployed and additional support capacity beyond nuclear weapons themselves. For example, increasing and sustaining the alert level of the bomber force would require an increased number of air crews and tanker availability. Similarly, the United States may need more submarines than are at sea day-to-day because maintenance and upgrade schedules restrict all submarines from always being at sea.

The central question is: What are the operational demands of achieving a particular force posture? More precisely, what are the operational requirements of increasing or decreasing the number of deployed *x* on *y* alert status (*x*

Defender with 5th Bomb Wing guards entry control point during Global Thunder 23, at Barksdale Air Force Base, Louisiana, April 14, 2023 (U.S. Air Force/James Thompson) representing the nuclear delivery system, *y* representing desired alert status)? The precise answer to most of these questions is not publicly available, but even outside analysts must consider the operational implications of any desired change in force posture—whether in number or alert status. Key questions include:

- What operational requirements must be met to present the nuclear force as desired?
- What is the desired alert posture of nuclear forces?
- If the force is generated, how long must/can it be operated in that state? How long will it take to regenerate afterward?
- How much of the force needs to be postured in a survivable mode at a given time?
- How much flexibility is needed in how nuclear operations are executed?

Conclusion

Primary U.S. competitors are augmenting their strategic capabilities and magnifying the salience of nuclear weapons in their national strategies. The resulting geopolitical risks are compounded by an unpredictable technological future and internal programmatic and operational risks relating to U.S. strategic forces. Within this context, the United States must continue meeting its deterrence and assurance objectives, retaining the ability to execute strategic force employment guidance, and navigating operational constraints. In devising approaches to such an amorphous strategic environment, analysts must reframe nuclear force sizing debates around fundamental disagreements and assumptions regarding the role of nuclear weapons in achieving U.S. national security objectives.

The proposed framework identifies four analytic dimensions (risk management; deterrence and assurance; strategic force employment; and operations), and key considerations therein, to structure debates about the appropriate attributes and characteristics of the U.S. nuclear force. Risk management approaches accentuate ways in which other instruments of national power can help mitigate geopolitical, technological, programmatic, and operational risks. Highlighting deterrence and assurance requirements focuses thinking on core objectives for U.S. strategic capabilities. The principles and policies shaping strategic force employment focus on the underlying requirements for nuclear weapons directed by U.S. leaders. Operational considerations require analysts to account for operational constraints of fielding a particular force composition.

Key questions across each dimension reveal important assumptions and differences in beliefs about the necessary attributes and characteristics of U.S. nuclear forces. By highlighting the component parts driving U.S. policy and strategy, analysts can structure conversations about U.S. nuclear forces in a way that maximizes their utility and policy relevance. Using such a framework is critical to ensuring that U.S. leaders understand the full ramifications of any changes to the composition of U.S. nuclear forces without getting lost in numbers debates. JFQ

Notes

[1] *The Nuclear Matters Handbook 2020* (Washington, DC: Department of Defense, 2020), 16, https://www.acq.osd.mil/ncbdp/nm/NMHB2020rev/docs/NMHB2020rev.pdf.

[2] "Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command," *Defense.gov*, April 30, 2021, https://www.defense.gov/news/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/.

[3] *National Security Strategy* (Washington, DC: The White House, October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[4] According to the *Report on the Nuclear Employment Strategy of the United States—2020* (Washington, DC: Department of Defense, 2020), "Nuclear weapons alone, no matter how capable, however, cannot have the necessary deterrence and assurance effects without a realistic and credible supporting strategy, tailored to potential adversaries," 4.

[5] *Military and Security Developments Involving the People's Republic of China 2023: Annual Report to Congress* (Washington, DC: Department of Defense, 2023), https://media.defense.gov/2023/oct/19/2003323409/-1/-1/1/2023-military-and-security-developments-involving-the-peoples-republic-of-china.pdf.

[6] *Military and Security Developments Involving the People's Republic of China 2022: Annual Report to Congress* (Washington, DC: Department of Defense, 2022), https://www.defense.gov/CMPR/.

[7] Hans M. Kristensen, Matt Korda, and Eliana Reynolds, "Russian Nuclear Weapons, 2023," *Bulletin of the Atomic Scientists* 79, no. 3 (2023), 179–199, https://doi.org/10.1080/00963402.2023.2202542.

[8] Hans M. Kristensen and Matt Korda, "North Korean Nuclear Weapons, 2022," *Bulletin of the Atomic Scientists* 78, no. 5 (2022), 273–294, https://doi.org/10.1080/00963402.2022.2109341.

[9] *Nuclear Posture Review 2018* (Washington, DC: Department of Defense, 2018), 2, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

[10] *U.S.–North Korea Relations*, IF10246 (Washington, DC: Congressional Research Service, April 29, 2020), https://crsreports.congress.gov/product/pdf/IF/IF10246/14.

[11] While the framework already considers geopolitical dynamics, this dimension is more narrowly focused on incorporating geopolitical change into overarching strategies and policies for risk management. Geopolitical and technological risks are primarily external risks, while operational and programmatic risks depend much more on internal risks stemming from U.S. political and military processes.

[12] National Security Action Memorandum 109, *U.S. Policy on Military Actions in a Berlin Conflict* (Washington, DC: The White House, October 23, 1961), https://www.jfklibrary.org/asset-viewer/archives/JFKNSF/332/JFKNSF-332-011.

[13] "30. Memorandum of Conversation," January–May 1961: Consideration of the Question of Germany and Berlin (Documents 1–31), in *Foreign Relations of the United States, 1961–1963*, vol. XIV, *Berlin Crisis, 1961–1962* (Washington, DC: Office of the Historian, May 31, 1961), https://history.state.gov/historicaldocuments/frus1961-63v14/d30.

[14] Charles Glaser, Austin Long, and Brian Radzinsky, eds., *Managing U.S. Nuclear Operations in the 21st Century* (Washington, DC: Brookings Institution Press, 2022).

[15] Ibid., 111.

[16] Ibid., 120.

[17] *Report on the Nuclear Employment Strategy of the United States—2020*, 6.

Chinese model promotes smartphone outside electronics center notorious for selling fake, gray market, and pirated electronics, in Beijing, September 27, 2015 (Stephen Shaver/UPI)

From "Made in China" to "Created in China"

Intellectual Property Rights in the People's Republic of China

By Gerald J. Krieger

Colonel Gerald J. Krieger, USA (Ret.), is an Independent Scholar. He holds a Ph.D. in International Relations from Salve Regina University.

Friction between the United States and the People's Republic of China (PRC) on technology captures the headlines regularly. American leaders discuss potential bans on U.S. investment in high-end Chinese tech companies involved with advanced semiconductors, artificial intelligence (AI), 5G technology, and quantum computing. U.S. leaders and the Taiwan Semiconductor Manufacturing Company recently announced that Taipei would invest $12 billion to open a semiconductor facility in Arizona to support 5G and other advanced technologies in the United States and revised the investment in late 2022 to include a second semiconductor chip plant for a total investment of $40 billion.[1] The first plant will produce 4-nanometer chips, while the second will produce the industry's most advanced chips at 3 nanometers to meet the U.S. annual demand of 600,000 wafers per year.[2]

The PRC's growing influence has generated a cottage industry of scholars and writers who do everything from explaining the inner workings of the Chinese Communist Party (CCP) to exposing threats posed by Chinese territorial ambitions and the pending eclipse of the United States as a global power. President Xi Jinping stated in 2014 that the first-mover advantage would go to "whoever holds the nose of the ox of science and technology innovation."[3] American leaders must better understand China's quest for technological superiority and intellectual property and continue modifying policies more aggressively.

Data indicate that the PRC continues to be guilty of flagrant intellectual property theft (IPT), forced technology transfers, and trademark and intellectual patent infringement (IPI). While it is outside the scope of this article, many factors are involved, and U.S. businesses might be partially responsible for lackadaisical agreements and protection processes in their quest for market access in China. Nevertheless, a 2016 report issued by the U.S. Chamber of Commerce Global Intellectual Property Center indicated that approximately 86 percent of counterfeit goods continued to emanate from the PRC.[4] Simply looking at China as the source of counterfeit products might suggest that IPT is rampant and that little has changed.

However, another aspect of China's growth is missed. The CCP is committed to leading and innovating in several high-tech sectors, which will continue to drive increased intellectual property (IP) protection for Chinese and foreign companies. The data support a shift toward greater protection of intellectual property and patents within the country. Chinese companies are becoming more protective of their IP, and there were three times as many IP-related lawsuits filed in 2020 as in 2016.[5] Hence, it is worth exploring the transformation of intellectual property rights (IPR) in China, particularly given the increased competition and restrictions on American high-tech products. This is driving China to find international and internal replacements to mitigate risks to Chinese interests.

This article focuses on progress in China's protection of intellectual property. Specifically, it looks at China's changes toward protecting IP as the PRC continues to drive economic growth as one of the world's leading economies. Today in China, the reality of IPT is somewhat more complex. Some Chinese companies that are global leaders—such as Huawei, with its 5G network chips—are built on government subsidies and nontariff barriers to create national champions under the protection of the state.[6] As James Lewis reported in 2020, China does not hesitate to use "unfair practices and policies to advance its firms, extract concessions, or block competition by foreign companies in China."[7] This has become more typical of foreign companies' challenges in China's markets.

The PRC has made significant progress toward greater IP protection and will continue to do so. However, it might not become an innovation hub because of stringent centralized control by the CCP. China's vast resources and population mean that the PRC will seize and dominate some sectors simply because of scale. Several implications for U.S. national security demand modification and substantial changes to American research and development (R&D) programs. Three suggestions are advanced herein to ensure America retains a competitive edge: increase funding to the Defense Advanced Research Projects Agency (DARPA); increase funding to university and college R&D programs; and expand and redefine the Advanced Robotics for Manufacturing Institute to follow the model (which is explored later) of Germany's Fraunhofer-Gesellschaft, which began in 1949 as a nonprofit organization and became one of the world's leading applied research organizations. A rudimentary historical framework helps us grasp the distinct differences in Chinese culture that are easily overlooked.

Background

Chinese education and administrative vocations historically focused on rote memorization in imperial China as early as the Tang dynasty during the late classic period (618–907 CE). During the imperial period, candidates had to pass an examination to demonstrate basic knowledge of Chinese classics to qualify for employment in government jobs. Memorizing information was prized, and original thoughts, synthesis, and analysis were not valued. Vestiges of the system still exist in the PRC and Taiwan (Republic of China). However, the influence of Marxism and Leninism and the importance of a single version of truth became the core of PRC society.

Furthermore, the Cultural Revolution (1966–1976) under Chairman Mao Zedong purged academics and innovative thinkers while promoting blind obedience to communist ideology, as presented by Mao. Taiwan charted a new democratic path that embraced capitalism, innovation, and global collaboration, and still does today. This explains why it is one of a handful of countries that dominates advanced microchips 7 nanometers and below.[8] It is worth noting that although China is the world's largest consumer of semiconductors and chips, it has yet to develop facilities to fabricate more advanced chips. The PRC relies on advanced chips from other countries to support its supplies.

Given China's historical focus on memorizing facts rather than critical thinking and creativity for its citizens, is it only natural that it was slow to catch on to the notion that ideas are the property of individuals? As Lawrence Page writes, "An arguable effect of these values is that the perceived need to protect IP is outweighed by the tendency toward placing collective duties above individual rights."[9] With the growth of industrial production in the 1980s and 1990s, China's developing economy snowballed through counterfeiting, mimicry, and reverse-engineering products to provide cheaper alternatives globally. One of the consequences of the practice was that many companies sought to make money quickly rather than build quality products and establish brand names and long-term relationships with consumers.[10]

Intellectual property primarily refers to *patents*, *copyrights*, *trademarks*, and *trade secrets*, though these terms are not mutually exclusive or easily defined. The U.S. relationship with China over trade imbalances and IP has been tense recently. It is easy to jump to conclusions and condemn China for insufficient IPR, but the details must be set in context. Ian Harvey and Jennifer Morgan point out, "All too often, fair concerns about the ability of Western companies to compete with Chinese ones, or fears about the outsourcing of production to take advantage of cheap labor, are miscategorized as IPR issues."[11] Although not plentiful, some studies have demonstrated that it is not uncommon for "complaints" from U.S. senior business executives to be based on a lack of understanding of IP, as well as their role in further exacerbating the problem in China, which can often be a result of weak patents and oversight in registering patents in China.[12] More detailed analysis helps sort the facts from fiction.

Transforming IP

Before 1984, patent laws did not exist in China. The growth of intellectual property in China made tremendous progress in the 1980s and 1990s, with Chinese representatives attending all international IPR conventions. Before this period, China was listed as one of the top violators of IP, driven mainly by movie and software violations. Numerous fines and court judgments imposed on Chinese companies—ranging from infringements on the Walt Disney Company's IPR by manufacturing and selling unlicensed products to 200,000 unlicensed copies of Microsoft's Disk Operating System—were common. However, the penalty did not outweigh the benefits in many cases. To cite one example, the fine for pirating was only $2,500.[13] Flagrant violations by Chinese companies continued to generate tensions with larger foreign companies. In the late 1990s, it was clear that Beijing was progressing toward raising standards and cleaning up trade practices to open markets worldwide. During this window, China began passing trademark laws (1982) and patent laws (1984), and establishing special IP courts in five regions: Hainan, Guangdong, Fujian, Beijing, and Shanghai.[14] The German government also helped China establish an electronic patent database in 1995. A software title verification office created in Beijing in May 1997 primarily served as a liaison for U.S. software companies. Subsequent revisions to China's copyright laws were expanded in 2001 to include online copyright protection.[15]

The U.S.-China agreement in December 2001 marked China's entry into the World Trade Organization (WTO), ushered in a wave of changes, and solidified the basis and guidelines for the Chinese socialized market. The PRC formed the General Administration of Quality Supervision, Inspection, and Quarantine department to assess 21,000 technical standards while revising 9,000 others to bring various industries in compliance with WTO rules.[16] However, central to China's entry into the world economy was maintaining a developing-country status that conveyed more lenient policies.[17] China corrected several unfair trade practices, but the CCP's desire to boost economic growth outweighed the anticipated costs. Entry into the WTO helped China's exports and increased participation in a larger global market, ultimately refining its competitive edge. The growth in Chinese exports is illustrative and showcases the Chinese transformation driven by its entry into the WTO, although the rapid growth created problems. In 1998, Chinese exports were USD 320 billion, surging to over USD 600 billion in 2005, though stimulating foreign direct investment in the Chinese economy also doubled to over USD 100 billion.[18]

The PRC's watershed moment for IP began in 2005, as it established the milestones of China's IP protection strategy. China's State Council announced the Intellectual Property Strategy Action Plan (2014–2020), which guided the goals and steps for program implementation.[19] The key objectives of the program were to increase China's creation of IP, enhance the integration of IP into the industry, improve the protection of IP, and create a system to manage it.[20] While the improvements in IP protection were noticeable, there were still several gaps and continued infractions.

One of the PRC's greatest challenges to IP protection is impossible to eradicate. The CCP is intrinsically tied to IP courts and the country's legal system. While the courts might not have complete autonomy, the Party will be forced to reduce corruption and respond to public demands. Although many changes have taken place in China, there will always be isolated pockets or areas difficult to control. For example, the Chinese city of Putian is known as the counterfeit-sneaker capital of the world, where corruption in courts and political interference by influential companies are ubiquitous, despite efforts to eradicate the problem.[21]

In 2015, Peter Yu wrote about reports of IPT in China: "As troubling as these developments have been, China has also slowly, and somewhat paradoxically, emerged as one of the world's leading intellectual property powers."[22] The riddle is more easily explained by the size of the Chinese government and the vast territory that must be monitored for violations. In other words, China is improving IPR, though its government structure hampers it. James Brander, Victor Cui, and Ilan Vertinsky note, "A key institutional characteristic of China that impairs adherence to international IP protection is the fragmented nature of its governance system. The central government, provincial governments, and individual ministries within government have competing and overlapping areas of authority."[23]

Assembly plant workers assemble engines at Geely Automobile Manufacturing Plant, March 14, 2017, Linhai, Zhejiang Province, China (Jenson/Shutterstock)

Despite this challenge, China continues to make regular improvements to IPR. Local government officials can find local consumer demands more compelling than the rules and regulations established by Beijing, invoking the famous Chinese expression, "The mountains are high, and the emperor is far away." Nevertheless, national interest drives the protection and enforcement of IPR, while China's strong central government provides a more responsive policy with fewer of the operational constraints present in the United States or Europe.

While China continues to be the home to manufacturing most of the world's counterfeits, it also has a long history of IPT and forced technology transfers as a condition for foreign companies to operate in China. According to the Office of the United States Trade Representative (USTR)'s April 2019 *Special 301 Report*, the Chinese government uses "joint venture requirements, foreign investment restrictions, and administrative review and licensing processes to force or pressure technology transfers from American companies."[24] While not all intellectual property is forced from companies, joint ventures between foreign and Chinese companies and foreign direct investment provide a mechanism to collect IP. Intellectual property covers various categories, including copyrights, trademarks, and is patents. China's focus on critical high-tech sectors began in 2015 as part of the 13th and 14th Five Year Plans, and is outlined in its Made in China 2025 (MIC2025) program, which focuses on innovation that dictates tighter IP protection.[25]

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organization provide critical documents for creating responsible IP regulation. Both recognize several types of intellectual property and rights, though most are captured in IP in motion pictures, art, literature, software, music, chemicals, and trademarked goods. Still, emerging technologies will force consistent revisions to these documents.[26] The PRC is shaping norms, as it has sponsored revisions to the TRIPS agreement shaping the nuances of future patents in biological and genetic research.[27] The PRC's MIC2025 seems to garner large shares of emerging technologies that encompass biological and genetic research.

In 2005, the PRC became the world leader in IP-related lawsuits, a trend that continues today. China's leadership in patent protection, coupled with its strong government and industry linkages, suggest more resources will be devoted to critical industries such as AI and robotics. China's creation of USD 1.55 trillion government guidance funds captures the scale of the problem and the volume of resources the CCP is devoting to technological innovation.[28]

Statistics published by the PRC's State Intellectual Property Office show increased patent infringement seizures and court cases. Additionally, litigation by foreign plaintiffs against Chinese defendants grew from 177 filings in 2006 to 745 cases in 2015.[29] For these reasons, a more thorough review of the nuances of IPT in China is crucial. At the same time, the number of registered patents in China highlights the progress and strides in patent protection.

Maglev train exiting Shanghai Pudong International Airport, China, on May 20, 2006 (Courtesy Alex Needham)

USTR's *Special 301 Report* placed China on the "Priority Watch List." The report cited examples of China committing intellectual property infringement and other concerns.[30] The USTR document recognized China's governmental changes, claiming that "China failed to make fundamental structural changes to strengthen IP protection and enforcement."[31] While the report captured a few bright spots, the details of IP changes in China are overlooked.

To stimulate innovation and entrepreneurs, China recognizes that it must protect these innovations from internal and external competitors by more effectively managing IP. In a meeting with the Politburo, Xi Jinping announced that China must have more robust laws to improve the business environment and strengthen IP rights domestically and abroad.[32] The PRC's technological innovation and MIC2025 hinge on innovation in critical high-tech sectors vulnerable to IPT and represent a threat to national objectives outlined by the CCP. MIC2025 was released in 2015 and reflected the CCP's 10-year plan to update Chinese manufacturing and focus on the top tier of value-additive manufacturing with more complex and sophisticated products. Many industries tie into the fourth industrial revolution that will integrate big data, cloud computing, and other emerging technologies into the global supply chain.[33] China is already leading in some areas, such as 5G technology. Peter Yu wrote in 2017, "Among corporate applicants . . . Huawei Technologies and ZTE Corporation had the world's first- and second-largest volumes of international patent applications, respectively."[34] At least in communications infrastructure, Chinese innovation appears among some of the top companies in the world.

As businesses expand into new areas, the CCP recognizes that IPT reduces company profits and might deter foreign and Chinese software companies from investing further in innovation directed at China's consumers. The PRC's commitment to acting as the leader in many high-tech industries underscores its voracious appetite for attaching strings to deals with Western companies to ensure that they sign technology transfers as a condition for doing business in China. America is not alone in facing challenges with doing business in China, and German lobbyists are vocal about the difficulties. However, the conversation has shifted from IP to forced technology transfer agreements, which appears to be expected as China attempts to comply with international norms.

Although it took place in 2001, an example of how Chinese companies interact with the West to conform to the law is illustrated by the German consortium ThyssenKrupp-Siemens (TKS).[35] TKS signed a contract with China to build a maglev (magnetic levitation) train with more than 200 kilometers of track at the cost of over EUR 20 billion. Shortly after starting the project, China demanded a significant discount due to technical issues with similar systems in Europe. Less than a year after the track was completed, Chinese technicians reverse-engineered the track and cars, producing an eerily similar prototype, canceling the more significant construction contract. Despite these frustrations, TKS eventually completed a much shorter (30-kilometer) track to the Shanghai airport and received a fraction of the quoted price.[36] These events capture the gauntlets many Western companies face when doing business in China. A 2019 U.S. Business Council survey produced only 5 percent of respondents who were approached about signing such agreements, suggesting that China's companies have become more subtle in acquiring foreign technology, representing a slight shift in policy to moving away from foreign direct investment.[37]

Nevertheless, the high-speed rail (HSR) example portends another challenge. Once China borrowed and reverse-engineered rail technologies, its HSR industries took off. The PRC created extensive rail networks and now is home to one of the largest and most modern global rail systems. Chinese companies also began to bid on international rail projects and undercut other countries. The net result is that between 2008 and 2014, China became the world leader in HSR, with over 11,000 kilometers of domestic track rated at speeds greater than 250 kilometers per hour.[38] Because of China's economies-of-scale advantage, it is now the industry leader, specializing in low-cost track installation and networks. The PRC has pioneered ultrafast networks with trains capable of traveling up to 360 kilometers per hour, all at a fraction of the cost of rival companies in Europe and North America.[39] The HSR industry might become increasingly common as China dedicates its vast economy and financial resources to other sectors.

Patents

China's commitment to becoming a technological leader and global innovator is driving an increase in registered patents, which stood at 13,751 in 1998, and with an astonishing 353,313 by 2012.[40] According to the World Bank, by 2019, Chinese patent applications more than tripled to 1,243,568.[41] While the sharp increase in patent applications does not necessarily translate into patent grants and true innovation, it does represent a trend. The number of registered patents increased by 122 percent between 1998 and 2012, reinforcing changes in China as the CCP attempts to stimulate innovation and establish a creative environment like that in the West. The World Intellectual Property Organization database highlights in 2022 that IP filings for Chinese residents were 1,464,605, though only 798,347 patents were granted.[42] This suggests that many patent applications are frivolous and useless for industry and consumers. The top Chinese patent applicants are Huawei, BOE Technology Group, Guang Dong Oppo Mobile Telecommunications, and ZTE Corporation, dwarfing all other patent applications.[43]

The sharp increase in patent applications comes with associated problems, as authors Brander, Cui, and Vertinsky highlight: "The large surge in patenting in China without developing a matching institutional capacity to examine patent applications properly contributes to patent thickets (that is, dense webs of overlapping rights), which increase litigation and reduce the system's capacity to protect legitimate IPRs."[44] According to the Congressional Research Service, in 2019 the United States led in the number of patent applications filed under the Patent Cooperation Treaty (PCT), an international patent system, with 52,005 PCT applications filed, but it was closely followed by China (with 50,563 applications) and Japan (with 47,888).[45] Intellectual property drives industrial growth and is an integral part of economic growth, higher wages, and exports, which are crucial to maintaining a competitive edge in the global economy.

In 2019, the PRC revised the trademark law and passed an anti–unfair competition law to prosecute those who leak trade secrets. In 2020, revisions to the patent law reduced the burden of proof for defendants, making it easier to file complaints with patent courts. Copyright law penalties for damages were raised tenfold to RMB 5 million (USD 773,000).[46] The importance of IP is not lost on China's leadership; the emphasis on fostering innovation and the need to protect Chinese entrepreneurs are partially responsible for increasing IPR disputes in China. IP lawsuits are rising in Chinese courts, among both Chinese and non-Chinese plaintiffs. For example, there were only 177 cases in 2006, but by 2015, the number of cases had grown to 745.[47] The numbers have increased dramatically over the past few years. In 2019, for instance, Chinese courts reported 22,722 new cases involving patent disputes, with 3,176 new IP cases filed with the highest court in China, the Supreme People's IP Court.[48]

China's recent quest to lead in key technology sectors outlined in MIC2025 will continue to drive changes to improve IP protection. The 10 industrial sectors that China is targeting are information technology (AI), robotics, green energy, aerospace, ocean engineering, railway equipment, power equipment, medical devices, agricultural machinery, and new materials (which involve chemistry, physics, and metallurgy).[49] Several Chinese companies are currently leaders in some of these technologies. A few examples are Baidu (AI and autonomous vehicles), SMIC (semiconductors), DJI, and Megvi (AI and drones). It should also be mentioned that many more Chinese companies are also applying to American and European patent offices.

Two conclusions are possible based on these challenges in China. One that appears the most likely is that China will naturally conform to international standards for IP once it creates the appropriately scaled institutional framework to support the workload and infrastructure. However, Brander, Cui, and Vertinsky make different predictions for the future of Chinese IP protection. They argue that the PRC will adopt international standards only once the Western world applies significant pressure, specifically through the TRIPS agreement, which must be updated and renegotiated.[50] The original agreement was established in 1995 and covered many types of IP, though technological innovation created new fields with the rapid growth of advanced technologies. The new agreement should specify what is and is not admissible for protection, mainly with the emerging field of biological entities. They correctly argue that as a global leader, China must be a stakeholder in all processes and negotiations involving international bodies and institutions.

IP protection must be balanced and implemented so that patents are not granted in a comprehensive manner that would stifle research and innovations, particularly in technological sectors. It is possible to create a rigid patent system where monopolies might be held by a large company that impedes innovation of other firms and future research while also stiffly regulating "patent trolls or assertion entities" that never produce anything tangible, impose taxes, and assess fees on companies.[51] Brander, Cui, and Vertinsky argue that standards for granting patents in the United States and China are too lenient and low, while a single standard needs to be modified as 20-year patent protection from the filing date might not make sense.[52] They miss the rapidly evolving high-tech industry that should be captured by a limited span, given the nature of the business and rapid transformation of some sectors. A 5-year window might be more viable.

The 2019 creation of an IP tribunal is a step in the right direction and allows appeals to local judgments to the Supreme People's Court through connections to high-level members of the CCP.[53] Reports show that as many as 19 more courts will be debuted soon.[54] An off-the-record case lodged by an American company against one of China's tech Brobdingnagians in a large city undermined this small win when local police omitted U.S. representatives from communications while negotiating privately with the court, and the case was dismissed.[55]

The future of IPR in China looks promising, though there are still challenges. Over the past few years, China has made tremendous strides to safeguard IP locally to protect Chinese entrepreneurs and globally by creating specialized IP courts, a Supreme Court IP tribunal, and a host of laws and regulations regarding IP.[56] However, Beijing's IP infrastructure is integrated into the legal system, which the CCP closely monitors. Another more potent criticism is that online infringement is more prevalent and harder to regulate. At the same time, China's lack of a "civil discovery process would mandate a philosophical shift in the country's legal system, one that would empower the plaintiff over the defendant. . . . So far, China has not indicated that it is willing to move in that direction."[57]

China's famous WeChat platform protects users from companies looking for infringement while allowing users to create multiple accounts to effectively generate anonymous transactions, which are difficult to track back to counterfeit product sales.[58] Nevertheless, developed regions of China reveal a court system of good quality, and the cost of IP litigation is a fraction of that in the United States. At the same time, judgments are often processed fast by international standards, with most resolved within a year.[59] In 2005, China became the world leader in IP-related lawsuits, a trend that continues today.[60] On further inspection, China's large economy is growing rapidly, and it is making changes to IP protection that are reasonable and consistent with any Western standards. The media and politicians depict China in an unfavorable light that ignores the tremendous strides made as the country takes the stage as one of the most powerful economies globally.

Some critics look at the Great Chinese Firewall and strict controls of the CCP and the tremendous focus placed on a homogeneous society that controls risk-taking and limits creativity. They conclude that such a culture can never truly be innovative, or at least that innovative breakthroughs that impact the world will be rare. This was the conclusion reached by Carly Fiorina, former chief executive officer of Hewlett-Packard from 1999 to 2005.[61]

Conclusion

While China is making strides in protecting IP and patent applications, the implications for U.S. companies are concerning. Intellectual property is the linchpin of innovation. American analysts should be less concerned with China's IPI issues and more mindful of internal changes and the strides the CCP is making toward safeguarding IP. China's increase in patent applications should be concerning and underscores the improvements inside China for greater IP protection. That Chinese entrepreneurs are also registering patents in the European Union and the United States is also an indication that change is brewing below the surface in China regarding IP. The roughly 20,000 new court cases involving patent disputes indicate a shift in the PRC. The creation of special IP courts, with 19 more planned, foretells further patent and intellectual rights protection in the country.

China's quest to be a global leader in emerging technology, such as AI and other high-tech industries (10 integral to the CCP's Made in China 2025 plan), means that it might succeed in many areas. While the United States has led in these technologies for many years, the CCP is focused on making strides in these sectors. Furthermore, the PRC is dedicating significant investment dollars to the program and allocation of "government guidance funds." These funds are public-private investments that, as of the first quarter of 2020, registered RMB 11 trillion (USD 1.55 trillion).[62] These funds are directed toward developing industries critical to the PRC's national security, from semiconductors to AI. In addition to special funds directed to R&D, the Chinese government offers direct subsidies and tax rebates to companies in key industries. China's advantage is that it can and will heavily fund these sectors, whereas the U.S. Government has outsourced much R&D to the private sector.

In the United States, the commercial sector drives much of the technological sector, while funding to defense agencies and research has waned. Due to IP concerns, many American companies are secretive with research programs and do not focus on the specialized military applications that support and address emergent military requirements. To bolster military applications to robotics and AI, the United States needs to increase DARPA's funding to at least $10.5 billion over the next 5 years, and it should be expanded along the so-called Fraunhofer model—a reference to the Fraunhofer-Gesellschaft—to focus on the warfighter and key emerging fields in applied science.[63]

The interests of U.S. companies and the government are often at odds. This is not a problem with authoritarian governments like China. In the United States, due to concerns about IP, some companies, such as Google (2015), elected not to renew contracts with the government. Google's actions were driven by its purchase of several robotic companies in 2013, though it continues to bid on some military contracts.[64] It has also declined

SAIC
中国商标金奖颁奖大会
CHINA TRADEMARK AWARDS CEREMONY
国家工商行政管理总局
State Administration for Industry and Commerce
世界知识产权组织
World Intellectual Property Organization
WIPO
中国·扬州
Yangzhou China June 30 , 2017

World Intellectual Property Organization Director General Francis Gurry speaks at Trademark Awards Ceremony in Yangzhou, China, June 30, 2017 (Courtesy Li Shiming)

to participate in Department of Defense robotics events, such as DARPA's robot-building contest, and refuses government funding.[65] Google has declined to share information and does not participate in and collaborate with the close-knit robotics community, which some critics suggest can slow the advancement of research in the field. China's government and centralized control mean that the country does not have to struggle as much against the competing interests of private companies.

While the United States needs to increase funding to DARPA, reinforcing and publicizing public-private partnerships would bolster American research efforts in crucial high-tech areas. America lacks a large organization like Germany's Fraunhofer-Gesellschaft that integrates the private and public sectors to concentrate on multiple areas of advancing applied science. However, there are a few examples, such as the Advanced Robotics for Manufacturing (ARM) Institute—one of the few large Federally funded collaborative projects focusing on manufacturing—though America needs more such programs. While ARM expanded to cover other areas and was instrumental in assisting the Department of Defense's response to the COVID-19 pandemic, it is insufficient to address emergent technologies and research growth.[66] However, if the program were expanded and altered, it could bolster American innovation and ensure that the United States retains leadership in vital technological sectors.

Better examples of private research partnerships with the government might only raise political hackles if the focus is on something other than the defense industry. Germany's use of research to stay relevant and retain jobs and manufacturing in the face of Chinese competition is helpful. While there are several factors at work, R&D programs bolster innovation and research for the industry.

One such program is the Fraunhofer model, which began in 1949 as a nonprofit organization and became one of the world's leading applied research organizations. According to the 2020 Fraunhofer Annual Report, the organization's 75 institutes and research units throughout Germany have 28,000 employees, operating with a research budget of EUR 2.8 billion (USD 3.6 billion).[67] It continues to expand, receiving a large portion of its income through industry and government projects. America needs a similar organization that an expanded ARM could fill, which would pay dividends specifically with applied research that overlaps with the MIC2025 core projects.

While expanding DARPA and increasing funding will help, it might not be enough to counter China's resources, such as the USD 1 trillion that the CCP allocated toward government guidance funds. University R&D is another area that has gradually increased from approximately $60 billion in 2007 to almost $77 billion in 2017, with half coming from the Federal Government.[68] The Federal Government can increase funding to colleges and universities, which peaked at 73 percent in the late 1960s and had ebbed and flowed to a level of 53.5 percent as of 2017.[69] In 2020, total R&D investments were at $708 billion, with $517.4 billion from business, $142.8 billion from the public sector, $22.6 billion from higher education, and $25.1 billion from nonprofit organizations.[70] A key opportunity is increasing funding from the government, which is quite low, hovering around 5 percent consistently since 2006.[71] Today, the private sector invests 3.6 times as much money as the U.S. Government. This leads to critical industries outsourcing elements of manufacturing to the lowest bidder in other countries. During the COVID-19 pandemic, American leaders and the public

Huawei display at Internationale Funkausstellung 2018, Berlin, September 2, 2018 (Courtesy Matti Blume)

became painfully aware of strained supply chains for medical supplies and drugs and of U.S. reliance on other countries. However, the lion's share of attention over the past few years has centered on the semiconductor industry. The danger of having high business R&D investment and low government investment, which Darrell M. West pointed out, is highlighted by these examples.[72]

In the upcoming geopolitical contest with China, it is crucial to remember American strengths. Several advantages include geography, the U.S. dollar as the world leader in currency reserves at 64 percent, and innovation with tech giants such as Google, Facebook, and Amazon. On the other hand, China is rapidly advancing with companies such as Baidu, Alibaba, and Tencent. The United States must make similar adjustments, while encouraging the private sector to participate and providing grants for research in areas where it wants to assume global leadership. Increased funding for military research and a return to expanded funding for DARPA could bolster American research in key high-tech sectors with military applications. China's leaders are dedicating over a trillion dollars to crucial industries. While the United States cannot match these investments dollar for dollar, we can leverage ingenuity and the inventive spirit that is the core of American culture if we start now.

While there continue to be IPR violations in China, China analysts need to be more mindful of China's rising influence in generating intellectual property. The reality is that China's growing influence in patent applications and innovation is the real threat. Although still relevant, China's intellectual property theft is a distraction and largely hype. Chinese companies will secure a larger share of patents in high-tech fields. This threat is real, while the PRC's IPT has largely evaporated. Urgent changes are necessary for U.S. R&D programs. Time is not on America's side. **JFQ**

Notes

[1] Leigh Hartman, "Taiwan's TSMC to Build $12 Billion Semiconductor Plant in the U.S.," *Share America*, May 20, 2020, https://share.america.gov/company-to-build-12-billion-semiconductor-plant-in-u-s/; Emma Kinery, "TSMC to Up Arizona Investment to $40 Billion With Second Semiconductor Chip Plant," CNBC, December 2, 2022, https://www.cnbc.com/2022/12/06/tsmc-to-up-arizona-investment-to-40-billion-with-second-semiconductor-chip-plant.html.

[2] Emma Kinery, "TSMC to Up Arizona Investment to $40 Billion With Second Semiconductor Chip Plant."

[3] As quoted in Jude Blanchette, "Xi's Gamble: The Race to Consolidate Power and Stave Off Disaster," *Foreign Policy*, July/August 2021.

[4] Global Intellectual Property Center, *Measuring the Magnitude of Global Counterfeiting: Creation of a Contemporary Global Measure of Physical Counterfeiting* (Washington, DC: U.S. Chamber of Commerce, November 2016), https://www.uschamber.com/assets/archived/images/documents/files/measuringthemagnitudeofglobalcounterfeiting.pdf.

[5] Maki Sagami, "China Goes on an Intellectual Property Offensive," *Nikkei Asia*, September 26, 2021, https://asia.nikkei.com/Business/China-tech/China-goes-on-an-intellectual-property-offensive.

[6] James Lewis, "Section 301 Investigation: China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation," Center for Strategic and International Studies, 2020, 2, http://www.jstor.com/stable/resrep24249.

[7] Ibid., 2.

[8] Elizabeth C. Economy, *The World According to China* (Medford, MA: Polity Press, 2022), 160.

[9] Lawrence Page, "Goodbye, Shanzhai: Intellectual Property Rights and the End of Copycat China," *University of Western Australia Law Review* 45, no. 1 (2019), 187.

[10] Ibid., 191.

[11] Ian Harvey and Jennifer Morgan, "Intellectual Property Rights in China: Myth Versus Reality," *E3G*, April 2007, 5, https://www.jstor.org/stable/resrep17742.

[12] Ibid.

[13] Sumner J. La Croix and Denise Eby Konan, "Intellectual Property Rights in China:

The Changing Political Economy of Chinese-American Interests," *World Economy* 25, no. 6 (June 2002), 764.

[14] Ibid., 761.

[15] Ibid., 762.

[16] Yeling Tan, "How the WTO Changed China: The Mixed Legacy of Economic Engagement," *Foreign Affairs*, March/April 2021.

[17] Hongyi Harry Lai, "Behind China's World Trade Organization Agreement With the USA," *Third World Quarterly* 22, no. 2 (2001), 237–255.

[18] Ibid., 250.

[19] George S. Yip and Bruce McKern, with Maja Schmitt, "Protecting Intellectual Property in China: Legal Provisions and Strategic Recommendations," in *China's Next Strategic Advantage: From Imitation to Innovation* (Cambridge, MA: MIT Press, 2016), 208.

[20] For a more detailed discussion of the program objectives and China's 12 target areas, see Yip and McKern, "Protecting Intellectual Property in China," in *China's Nex Strategic Advantage*.

[21] Daniel Rechtschaffen, "How China's Legal System Enables Intellectual Property Theft," *The Diplomat*, November 11, 2020, https://thediplomat.com/2020/11/how-chinas-legal-system-enables-intellectual-property-theft/.

[22] Peter K. Yu, "The Rise of China in the International Intellectual Property Regime," in *Handbook on the International Political Economy of China*, ed. Ka Zeng (Cheltenham, UK: Edward Elgar Publishing, 2019), 420, https://www.elgaronline.com/edcollbook/edcoll/9781786435057/9781786435057.xml.

[23] James A. Brander, Victor Cui, and Ilan Vertinsky, "China and Intellectual Property Rights: A Challenge to the Rule of Law," *Journal of International Business Studies* 48, no. 7 (July 2017), 915.

[24] Cited in Sean O'Connor, *How Chinese Companies Facilitate Technology Transfer from the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, May 6, 2019), 4.

[25] *Made in China 2025: Global Ambitions Built on Local Protections* (Washington, DC: U.S. Chamber of Commerce, 2017), 10, https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

[26] Brander, Cui, and Vertinsky, "China and Intellectual Property Rights," 909.

[27] For more details, see Yu, "The Rise of China in the International Intellectual Property Regime," 429.

[28] Ngor Luong, Zachary Arnold, and Ben Murphy, *Chinese Government Guidance Funds: A Guide for the Perplexed* (Washington, DC: Center for Security and Emerging Technology, March 2021), 3, https://cset.georgetown.edu/publication/chinese-government-guidance-funds/.

[29] Brander, Cui, and Vertinsky, "China and Intellectual Property Rights," 910.

[30] Office of the United States Trade Representative (USTR), *Special 301 Report* (Washington, DC: USTR, April 2019), 12, https://ustr.gov/sites/default/files/2019_Special_301_Report.pdf.

[31] Ibid., 40.

[32] Matt Ho, "Chinese President Xi Jinping Says Intellectual Property Protection Is Key Part of Country's Development Plans," *South China Morning Post* (Hong Kong), February 2, 2021, https://www.scmp.com/news/china/politics/article/3120118/chinese-president-xi-jinping-says-intellectual-property.

[33] James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations*, May 13, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

[34] Yu, "The Rise of China in the International Intellectual Property Regime," 425.

[35] Gabriela Pleschová, "The European Union and China: Economic Priorities of the EU in China and Their Institutional Support," *International Issues & Slovak Foreign Policy Affairs* 16, no. 3 (2007), 23.

[36] Ibid.

[37] Yukon Huang and Jeremy Smith, "China's Record on Intellectual Property Rights Is Getting Better and Better," *Foreign Policy*, October 16, 2019, https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/.

[38] Adam Tooze, *Crashed: How a Decade of Financial Crises Changed the World* (New York: Viking, 2018), 245.

[39] Ibid., 245.

[40] "Patent Applications, Residents," The World Bank, 2023, https://data.worldbank.org/indicator/IP.PAT.RESD.

[41] Ibid.

[42] "Intellectual Property Statistical Country Profile 2021, China," World Intellectual Property Organization, March 2023, https://www.wipo.int/edocs/statistics-country-profile/en/cn.pdf.

[43] Ibid.

[44] Brander, Cui, and Vertinsky, "China and Intellectual Property Rights," 916.

[45] Shayerah Ilias Akhtar and Liana Wong, *Intellectual Property Rights and International Trade*, RL34292 (Washington, DC: Congressional Research Service, May 12, 2020), 5, https://crsreports.congress.gov/product/pdf/RL/RL34292.

[46] Sagami, "China Goes on an Intellectual Property Offensive."

[47] Brander, Cui, and Vertinsky, "China and Intellectual Property Rights," 910.

[48] Matt Ho, "Intellectual Property: China's Evolution from 'Norm Taker' to 'Norm Setter,'" *South China Morning Post*, May 5, 2021, https://www.scmp.com/news/china/politics/article/3131750/intellectual-property-chinas-evolution-norm-taker-norm-setter.

[49] McBride and Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?"

[50] Ibid. The TRIPS agreement became effective on January 1, 1995. It is considered the most comprehensive multilateral agreement on intellectual property. For more information, see "Overview: The TRIPS Agreement," World Trade Organization, https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

[51] Brander, Cui, and Vertinsky, "China and Intellectual Property Rights," 917.

[52] Ibid.

[53] Huang and Smith, "China's Record on Intellectual Property Rights Is Getting Better and Better."

[54] Ibid.

[55] As referenced in Huang and Smith, "China's Record on Intellectual Property Rights Is Getting Better and Better."

[56] Rechtschaffen, "How China's Legal System Enables Intellectual Property Theft."

[57] Ibid.

[58] Ibid.

[59] Harvey and Morgan, "Intellectual Property Rights in China," 6.

[60] Huang and Smith, "China's Record on Intellectual Property Rights Is Getting Better and Better."

[61] Carly Fiorina, *Rising to the Challenge: My Leadership Journey* (New York: Sentinel, 2015), 75.

[62] Luong, Arnold, and Murphy, *Chinese Government Guidance Funds*, 3.

[63] "Budget," Defense Advanced Research Projects Agency, https://www.darpa.mil/about-us/budget.

[64] Doug Cameron and Alistair Barr, "Google Snubs Robotics Rivals, Pentagon," *Wall Street Journal*, March 5, 2015.

[65] Ibid.

[66] "Public-Private Partnerships Driving Science, Research Efforts," *Federal News Network*, January 15, 2021, https://federalnewsnetwork.com/federal-insights/2021/01/public-private-partnerships-driving-science-research-efforts/.

[67] *Annual Report 2020: For a Secure Future: Resilience Through Innovation* (Munich: Fraunhofer-Gesellschaft, January 2021), https://www.archiv.fraunhofer.de/Fraunhofer_Annual_Report_2020/#2.

[68] "R&D at Colleges and Universities," American Association for the Advancement of Science (AAAS), 2023, https://www.aaas.org/programs/r-d-budget-and-policy/rd-colleges-and-universities.

[69] Ibid.

[70] Darrell M. West, "R&D for the Public Good: Ways to Strengthen Societal Innovation in the United States," *Brookings Institution*, October 10, 2022, https://www.brookings.edu/research/rd-for-the-public-good-ways-to-strengthen-societal-innovation-in-the-united-states.

[71] "R&D at Colleges and Universities," AAAS.

[72] West, "R&D for the Public Good."

Special Amphibious Reconnaissance Corpsmen assigned to November Company, 3rd Raider Battalion, provide tactical combat casualty care training to Soldiers of 1st Battalion, 102nd Cavalry Regiment, during routine deployment to Somalia, August 24, 2019 (U.S. Navy/Patrick W. Mullen III)

The "Survival Chain"

Medical Support to Military Operations on the Future Battlefield

By Jennifer M. Gurney, Jeremy C. Pamplin, Mason H. Remondelli, Stacy A. Shackelford, Jay B. Baker, Sean P. Conley, Benjamin K. Potter, Travis M. Polk, Eric A. Elster, and Kyle N. Remick

Colonel Jennifer M. Gurney, USA, is Director of the Department of Defense (DOD) Joint Trauma System. Colonel Jeremy C. Pamplin, USA, is Director of the Telemedicine and Advanced Technology Research Center Headquarters. Second Lieutenant Mason H. Remondelli, USA, is an MD Candidate at the Uniformed Services University (USU). Colonel Stacy A. Shackelford, USAF, is the Trauma Medical Director at the Defense Health Agency. Colonel Jay B. Baker, USA, is Director of the DOD Joint Trauma Center, Combatant Command Trauma Systems Branch. Captain Sean P. Conley, USN, is an Assistant Professor at USU. Colonel Benjamin K. Potter, USA, is Professor and Chairman of the School of Medicine at USU. Captain Travis M. Polk, USN, is Director of the DOD JPC-6 Combat Casualty Care Research Program. Captain Eric A. Elster, USN (Ret.), is Professor and Dean in the School of Medicine at USU. Colonel Kyle N. Remick, USA (Ret.), is Professor of Surgery and Associate Chair for Operations at USU.

In *The Kill Chain: Defending America in the Future of High-Tech Warfare*, author Christian Brose describes a concept in which the speed that a combat force is effective at "closing the kill chain" will determine whether it wins or loses.[1] Brose proposes a redesign of our military combat infrastructure to "understand, decide, and act" faster than the enemy to employ the required force (for example, lethal versus nonlethal) to achieve *operational overmatch*. Following his lead, we propose the concept of a "survival chain" as the medical equivalent that could provide combat casualty care support to the "kill chain" to gain and maintain *medical overmatch* on future battlefields.

The Department of Defense Joint Trauma System (JTS) was created to provide optimal care to the wounded on a battlefield. The current National Defense Strategy anticipates future threats of large-scale combat operations (LSCO) against peer adversaries that may limit overall freedom of maneuver for medical evacuation, increase survivability risk of medical units, and limit timeliness and robustness of critical medical logistics. Thus, the JTS must continue to evolve and embrace the concept of Medical Performance Optimization (MPO) to adapt to this new operational reality.

MPO captures the intent of the JTS as a "continuously learning health system" to evolve the speed at which it can cycle through near-real-time data capture, analysis, and adaptation of knowledge and material solutions to optimize battlefield trauma care. Like the "understand, decide, and act" of the kill chain, JTS MPO will be the survival chain that relies on rapidly closing the JTS MPO cycle via "observe, orient, decide [or understand], and act" (the JTS OODA loop).[2] Therefore, the purpose of this article is to inform military leadership about the risks to optimal combat casualty care in potential future LSCOs and to provide a focused discussion of potential solutions to gain and maintain medical overmatch in the survival chain on the 21st-century battlefields.

Reframing Current Challenges

Casualty care on the battlefield is based on the JTS performance improvement cycle (MPO) overlaid on the North Atlantic Treaty Organization's Roles of Care guidelines.[3] The JTS mission includes overall clinical care optimization of the battlefield trauma system by providing clinical data collection and analysis, "loop closure" feedback to medical commands, identification of gaps in knowledge and skills for further research, best practice clinical guidelines, quality improvement, and informing education/training.[4] The JTS MPO process must continuously and rapidly optimize battlefield trauma care—that is, continuously enhance the survival chain to gain and maintain medical overmatch to address the volume of casualties expected for an LSCO.

The crux of the current challenge is that the past two decades of war in the Middle East have resulted in the focus on a conflict in which there are robust medical resources, fixed Role 3 combat support (*Role 3 facilities* are equivalent to multidisciplinary general hospitals), field hospitals in relatively safeguarded locations, as well as a hierarchical trauma system in which casualties move along a continuum of care with increasing capability at each level of care (figure 2).

The JTS performed well in the recent conflicts, but the reality of future land or maritime LSCOs drives the challenges we now face to prepare the system to deliver the excellent care expected from our Servicemembers and our nation. Data integration and technology are integral to MPO for our system to observe (collect real-time, relevant data), orient (or understand via rapid data analysis), decide (increase speed and accuracy of decisions), and act (treat casualties) to meet the expectation of leaders to decrease force attrition from injury and maximize its lethality. As Brose notes, "The problems facing the U.S. military are now taking on a fundamentally different and greater sense of urgency, and it goes beyond emerging technologies."[5]

The goal of the JTS in preparing for LSCOs is a more effective survival chain not only to provide new technologies that improve the deployed medical system but also to continue to evolve the current system by enhancing real-time data acquisition for MPO. As Brose describes for increasing lethality, solutions that improve survival and force regeneration may involve novel medical innovations, new mechanisms by which to deliver already proven medical interventions, and modernization of trauma medical systems involving nontraditional architectures that are not platform-centric.[6] Therefore, in this article, we focus on the three most urgent challenges to providing a survival chain in support of future military operations:

- point-of-injury care
- casualty evacuation care
- surgical care.

Challenge 1: Point-of-Injury Care

Initial casualty care at the classic Role 1 (*Role 1 care* includes medical treatment, initial trauma care, and forward resuscitation) will face many challenges that are typical of a force-on-force battlespace.[7] We know from data developed during the war on terror that most preventable deaths (88 percent) occur in the *field*, that is, the time between the point of injury to the first treatment facility (Role 2).[8] Therefore, the challenges during this phase of trauma care will be essential to illuminate gaps in education, training, and research to gain overmatch in LSCOs.

Main Risks and Potential Mitigating Measures During Point-of-Injury Casualty Care.

- Death from massive bleeding
  - Increase Tactical Combat Casualty Care training for nonmedical personnel to control hemorrhaging and free up line medics to care for the more seriously wounded
  - Train and equip combat medics for blood transfusion, walking blood banks, and additional hemorrhage control techniques and simultaneously develop novel technological solutions for bleeding control and delivering blood[9]
  - Develop novel antishock drugs, blood products or alternatives, and advanced clotting technology to mitigate combat deaths from hemorrhage.[10]
- Large casualty volume
  - Ensure more sophisticated training for combat medics on knowledge

Soldiers assigned to Army Reserve participate in Tactical Casualty Combat Care course at Joint Base McGuire-Dix-Lakehurst, New Jersey, September 10, 2023 (U.S. Air Force/Matt Porter)

and skills in triage (the sorting of casualties by the severity of injury) involving an intentional transition from optimal care for each individual casualty to "the greatest good for the greatest number" in mass casualty incidents (when the number of casualties outstrips resources available)[11]
- Develop simpler and more functional models for triage that may involve swift identification of those who are ambulatory or dead first, then stable or unstable, and increasing knowledge of resources readily available to the triage team[12]
- Develop best practices in the care of the injured in mass casualty incidents to clear the battlefield of hundreds (or thousands) of casualties and simultaneously provide care and maximize the force.

- Lack of resources
  - Integrate remote-piloted aircraft or other technology for medical logistics support in denied and hostile environments
  - Develop clinical decision-support tools for personnel working with limited medical resources
  - Develop real-time monitoring and decision support tools for medical assessments and interventions.

Challenge 2: Casualty Evacuation Care

The next phase of care conventionally involves the movement of casualties from the immediate area of active conflict to one that can render more advanced trauma care and damage control resuscitation. However, during a large-scale force-on-force fight with adversaries that possess comparable long-range fire technology and airpower, challenges might arise that could diminish this potentially lifesaving evacuation capability. As a result, this phase of care, still classically considered Role 1 care, will include Prolonged Casualty Care (PCC) through eventual medical evacuation when available.[13] In this phase, medics will be faced with caring for casualties beyond doctrinal timelines with large volumes of casualties and resource constraints—in other words, more complex care with less resources.

Main Risks and Potential Mitigating Measures to Casualty Evacuation and Prolonged Casualty Care.

- Denied operating environment
  - Increase knowledge and skills required by combat medics to perform PCC to extend typical hold and evacuation times until a more advanced resuscitation and surgical care capability can arrive or be reached[14]
  - Develop the means to employ telehealth and decision support in austere environments to augment medical care further forward
  - Improve clinical data capture through real-time, automated documentation for ongoing care and for MPO.

- Risk of air maneuver/ground movement
  - Develop automated medical care technology for aerial and ground vehicles and include environmental surveys for railways as a potential means for medical evacuation of large numbers of casualties
  - Employ remote-piloted aircraft for medical resupply to include blood products that could be delivered on demand to forward locations
  - Evolve Patient Evacuation Coordination Cells that include real-time, intelligent tasking that accounts for both clinical and operational factors in optimal timing and destination for patient movements.

- Lack of communication/command and control
  - Develop counter-electronic/counter–cyber warfare technologies to protect and ensure clinical and operational medical communications are available and not compromised
  - Consider a battlefield medical command and control element, linked with the JTS, with real-time situational awareness of the battlefield and, with oversight to best match patient evacuation timing, clinical care required, as well as the right destination medical capability for the best outcomes
  - Develop a method of automated, real-time tracking of casualties across the battlespace.

Challenge 3: Surgical Care

Although most combat casualties who succumb to their injuries do so at Role 1 before they arrive at a surgical capability, the concept of Role 2 and Role 3 care remains critical to the remainder of survivable injuries.[15] Without damage control and definitive surgery, a casualty may initially survive but then die of bleeding or long-term trauma complications, such as infection and organ failure. For example, a casualty with a bleeding liver may receive the appropriate initial treatment to prolong life until reaching a facility capable of surgery, but that injury could only be more definitively controlled by a surgeon opening the abdomen and manually controlling the ongoing bleeding. Due to this situation, survival will be compromised without timely surgical intervention. However, on the potential peer contingency battlefield, Role 2 facilities and advanced surgical teams will face challenges.

Risks and Potential Mitigating Measures for Initial Lifesaving Surgical Care.

- Operational training/interoperability
  - Re-emphasize organizing, training, and equipping small surgical teams that could optimally perform as both a surgical team and as an operational element[16]
  - Optimize surgical teams that have access to work together in high-volume trauma centers and conduct specific training to attain the clinical and operational capability required
  - Conduct research and data analysis to better understand what capability is required and how

- to best employ surgical teams in future operations
  - Improve the ability of surgical teams to capture data in future operations to be used for MPO.

- Maintaining casualty care expertise
  - Increase opportunities for deploying medical personnel to work individually and as teams in military Medical Treatment Facilities or in military-civilian partnerships
  - Continue to leverage the Joint Knowledge, Skills, and Abilities Program Management Office as the means to measure clinical specialty-specific medical readiness and provide clinical deployment readiness assessments
  - Research and develop technology that could augment clinical care through telementoring, telerobotics, augmented reality, or other emerging solutions.

- Risk of far-forward-deployment
  - Consider surgical teams with doctrine akin to a quick reaction force with the capability to move on the battlefield alongside operational elements to mass for casualty care at decisive points and then disperse when complete to minimize the risk of exposure
  - Establish international partnerships in geostrategic locations that could then be leveraged as a regional trauma capability while minimizing our military footprint[17]
  - Research and develop telesurgery capability for far-forward surgical locations to limit risk to surgeons and medical teams.

Conclusion: Closing the Survival Chain to Support the Kill Chain

The JTS has proved its effectiveness at decreasing death on the battlefield since its inception in 2005, and thus the organization was codified into doctrine in 2016. While the JTS provided tremendous advances over the past 20 years in combat, the next conflict might last for less than 2 years but have 10 times as many combat casualties as the last two decades. The JTS must continue to evolve through its MPO cycle to meet these anticipated challenges, most urgently for point-of-injury care, care during casualty evacuation, and surgical care as discussed.

We must actively seek to maintain our ability to optimize survival on the battlefield by decreasing warfighter attrition and thus producing the operational effect of maintaining combat strength. This is the mission of the Joint Trauma System. With the support of military leadership, the JTS could continue to evolve to support this critical role. The MPO concept is the cycle of near-real-time data collection and analysis, novel knowledge and/or material solutions, and rapid integration into battlefield trauma care (the JTS OODA) that would enable the JTS to adapt and react quickly when needed. By leveraging the existing processes of MPO and enhancing its speed of loop closure, the JTS would provide the survival chain that could gain and maintain medical overmatch on future battlefields regardless of the challenges presented. **JFQ**

Notes

[1] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020).

[2] Ibid.

[3] Allied Joint Publication (AJP) 4.10(A), *Allied Joint Medical Support Doctrine* (Brussels: North Atlantic Treaty Organization, May 30, 2011), https://shape.nato.int/resources/site6362/medica-secure/publications/ajp-4.10(a).pdf.

[4] Jeffrey Bailey et al., eds., *The Joint Trauma System: Development, Conceptual Framework, and Optimal Elements* (Fort Sam Houston, TX: U.S. Army Institute of Surgical Research, January 2012), https://jts.health.mil/assets/docs/publications/Joint_Trauma_System_final_clean2.pdf.

[5] Brose, *The Kill Chain.*

[6] Ibid.

[7] AJP 4.10(A).

[8] Brian J. Eastridge et al., "Death on the Battlefield (2001–2011): Implications for the Future of Combat Casualty Care," *Journal of Trauma and Acute Care Surgery* 73, no. 6 (December 2012), S431–S437, https://doi.org/10.1097/TA.0b013e3182755dcc.

[9] Andrew D. Fisher et al., "Low Titer Group O Whole Blood Resuscitation: Military Experience from the Point of Injury," *Journal of Trauma and Acute Care Surgery* 89, no. 4 (October 2020), 834–841, https://doi.org/10.1097/TA.0000000000002863.

[10] Jonathan J. Morrison, Joseph J. Dubose, and Todd E. Rasmussen, "Military Application of Tranexamic Acid in Trauma Emergency Resuscitation (MAT-TERs) Study," *Archives of Surgery* 147, no. 2 (February 2012), 113–119, https://jamanetwork.com/journals/jamasurgery/article-abstract/1107351; I. Roberts et al., "The CRASH-2 Trial: A Randomised Controlled Trial and Economic Evaluation of the Effects of Tranexamic Acid on Death, Vascular Occlusive Events and Transfusion Requirement in Bleeding Trauma Patients," *Clinical Governance: An International Journal* 18, no. 3 (July 2013), https://doi.org/10.1108/cgij.2013.24818caa.005.

[11] Stacy A. Shackelford et al., "Evidence-Based Principles of Time, Triage and Treatment: Refining the Initial Medical Response to Massive Casualty Incidents," *Journal of Trauma and Acute Care Surgery* 93, no. 2S Suppl 1 (August 2022), S160–164, https://doi.org/10.1097/ta.0000000000003699.

[12] Ibid.

[13] "Prolonged Casualty Care Guidelines: Joint Trauma System," *JTSHealth.mil*, December 21, 2021, https://jts.health.mil/assets/docs/cpgs/Prolonged_Casualty_Care_Guidelines_21_Dec_2021_ID91.pdf.

[14] Nedas Jasinskas, Regan Lyon, and Jay Baker, "Unconventional Warfare Medicine Is the Ultimate Prolonged Field Care," *Medical Journal (Fort Sam Houston, TX)*, no. Per 22-04-05-06 (April–June 2022), 27–31.

[15] AJP 4.10(A).

[16] Jay B. Baker et al., "Austere Resuscitative and Surgical Care in Support of Forward Military Operations—Joint Trauma System Position Paper," *Military Medicine* 186, no. 1–2 (January–February 2021), 12–17, https://doi.org/10.1093/milmed/usaa358.

[17] Regan F. Lyon, "When the 'Golden Hour' Is Dead: Preparing Indigenous Guerrilla Medical Networks for Unconventional Conflicts" (Master's thesis, Naval Postgraduate School, December 2021), https://calhoun.nps.edu/handle/10945/68685.

General Darryl Williams, commander of U.S. Army Europe and Africa and commander of NATO's Allied Land Command, right center, discusses mission command execution with senior officers from NATO HQ Allied Rapid Reaction Corps during Steadfast Jupiter 23, October 18, 2023 (U.S. Army/Kyle Larsen)

Converting a Political- to a Military-Strategic Objective

By Milan Vego

Political objectives are usually achieved by using one's military power. Converting political objectives into achievable military-strategic objectives is the primary responsibility of military-strategic leadership. This process is largely an art rather than a science. There are many potential pitfalls because much depends on the knowledge, understanding, experience, and judgment of military-strategic leaders. Most often, mistakes made are only recognized after setbacks or defeats suffered during the hostilities. Despite its critical importance, there is no consensus on the steps and methods in converting political- into military-strategic objectives. There is scant writing on the subject in either doctrinal documents or professional journals.

Political vs. Military Objectives

Any war is fought to achieve certain *political objectives*, which may be described as securing important national or alliance/coalition interests in a certain part of a theater. When aimed to achieve national interests, a political objective is strategic in scale. Its accomplishment could have a radical effect on the course and outcome of a war. In his seminal work *On War*, Carl von Clausewitz (1780–1831) wrote that "no one starts a war—or rather, no one in his senses ought to do so—without first being clear in his mind what he intends to achieve by that war and how he intends to conduct it. The former is the political purpose; the latter its operational objective."[1] He observed

Milan Vego is Admiral R.K. Turner Professor of Operational Art at the U.S. Naval War College.

that "the political object—the original motive for war—will thus determine both the military objective to be reached and the amount of effort it requires."[2] Political objectives may be purely political. However, they are often combined with ideological, geopolitical, economic, financial, social, ethnic, and religious objectives.

A *military-strategic objective* is ending the enemy's organized resistance and thereby achieving a major part of a given political-strategic objective. Yet the entire political objective is not accomplished unless military-strategic success is consolidated during the posthostilities (or stabilization) phase of a war. A military-strategic objective must *always* be subordinate to a given political objective. The British theoretician B.H. Liddell Hart cautioned that political leadership must make sure that political objectives of a war are achievable with military means that are currently or will soon be available. He warned that policy should "not demand what is militarily—that is, practically, impossible." The "war aims must be adopted to limitations of strength and policy."[3]

In the case of continent-size countries, such as the United States or the Russian Federation, or of the oceanic theaters (for example, the Atlantic or Pacific), the possibility exists of having a war in two or more war theaters. Then, for each of them, a single military-strategic objective must be determined. In World War II, the United States had two national military-strategic objectives: unconditional surrender of the Axis powers in Europe (Nazi Germany and Italy) and in the Pacific region (Imperial Japan).[4] Then, in each theater of war, there would also exist two or more *theater-strategic objectives*—whose accomplishment would result in the destruction of a major part of the enemy forces and then set conditions for a posthostilities phase in a given theater of operations. Their accomplishment would have a radical effect on the course and outcome of a war in a given theater. It would also signify a major phase in a war. In a theater of operations with a large population and developed infrastructure ("developed" theater), such as was Western Europe in World War II or the Iraqi theater of operations in 2003, the theater-strategic objective is subordinate to a given political objective (which, in turn, is subordinate to the national or alliance/coalition political-strategic objective) (see figure 1). In contrast, in a sparsely populated theater with little or no infrastructure ("undeveloped" theater), as were the Solomons, central Pacific, and Papua New Guinea in World War II, the theater-strategic objectives would be predominantly or exclusively military.

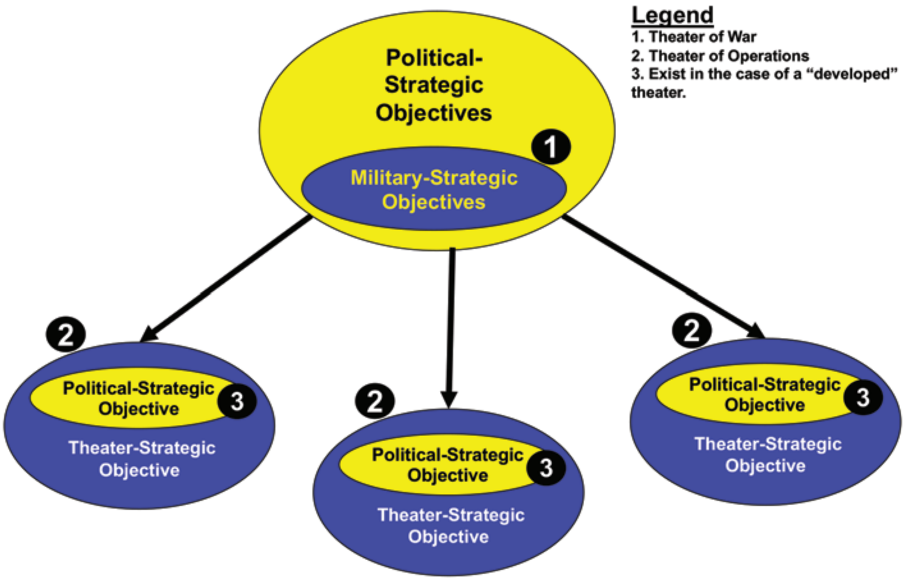
In the offensive phase of the war in the Pacific (after August 1942), the Allies had in the Pacific Ocean area three theater-strategic objectives: defending Alaska and the Aleutians, capturing the Solomons archipelago, and capturing the Japanese strongpoints in the central Pacific. In the Southwest Pacific area, the Allies had two identifiable theater-strategic objectives: capturing Papua New Guinea and the Philippines. The final theater-strategic objective for the Pacific Ocean area command was capturing/neutralizing the southern approaches to the home islands (Formosa, Iwo Jima, and Ryukyus) and then, jointly with the Southwest Pacific area's forces, assaulting and occupying the home islands. This part of the theater-strategic objectives was made unnecessary after atomic bombs were dropped on Hiroshima and Nagasaki in August 1945.

Prerequisites

Among the main requirements for determining a realistic military-/theater-strategic objective are sufficient military capabilities, sound prediction of the duration of a war, accurate strategic intelligence, and realistic political/military assumptions. The accomplishment of a military-strategic objective is predicated on having sufficient military capabilities. The greater one's numerical/qualitative superiority, the more ambitious the military-strategic objectives that might be accomplished. For German Field Marshal Helmuth von Moltke, Sr., the main requirement for a war was numerical superiority of the Prussian armies. This was achieved by general conscription. Moltke's aim was to defeat an enemy army in a "single powerful blow." At the same time, the importance of numerical superiority should not be overstated. Experience shows that in many cases, superior numbers are of no avail.

In evaluating overall strength of friendly and enemy forces, a great deal of attention must be paid to intangible elements, such as morale and discipline, will to fight, skills of the leaders, and soundness of doctrine. These factors are often more critical than numerical strength. Sometimes, the spiritual strength of an army may balance other

Figure 1. Military Theater-Strategic Objectives


Legend
1. Theater of War
2. Theater of Operations
3. Exist in the case of a "developed" theater.
Political-Strategic Objectives
1
Military-Strategic Objectives
2
Political-Strategic Objective
3
Theater-Strategic Objective
2
Political-Strategic Objective
3
Theater-Strategic Objective
2
Political-Strategic Objective
3
Theater-Strategic Objective

deficiencies. The influence of a single personality may also greatly enhance the capabilities of the entire army and even the entire state.[5] Experience shows that numerically weaker forces could often defeat a much larger force because of the better quality of their leaders and the better training, morale, and discipline of their troops. In Germany's invasion of France, Belgium, the Netherlands, and Luxembourg in May 1940, for instance, the ratio of attacker to defender was 0.7 to 1, or 3,740,000 Allied soldiers (including 2,240,000 French troops) facing 2,760,000 Germans. The Allies had a 3-to-2 superiority in artillery pieces. However, France had only 3 armored divisions (plus 1 more created during the campaign) against Germany's 10 panzer divisions.[6] The German success in that campaign was due more to much higher quality of leadership, doctrine, combat training, and morale/discipline than to materiel.

In some cases, as the war on the Eastern Front in 1941–1945 illustrates, the sheer number of troops, tanks, guns, and aircraft is simply overwhelming, no matter what the skills of the commanders and rank and file, morale and discipline, or training and soundness of doctrine of the opposing force. The Germans had assigned 145 divisions (including 19 panzer divisions and 14 infantry motorized divisions) with 3.2 million men (out of a total 3.8 million) for the invasion of Soviet Russia in June 1941.[7] They also had a small contingent of Romanian and Finnish forces, but the effectiveness of their equipment and combat was well below that of the Germans.[8] The German Eastern Army (Ostheer) was superior in combat experience to the Red Army. Except for nine security divisions (Sicherungs-Divisionen),[9] all other German divisions were fully equipped with modern weapons. The training and confidence of the German troops were high. German leadership, especially at the operational level, was superior to leadership of the Red Army.[10] The German high commanders were experienced in maneuvering large, motorized forces, and the individual German soldier was self-confident. The Germans believed that the element of surprise in launching the invasion would probably compensate for some of the German numerical inferiority.[11]

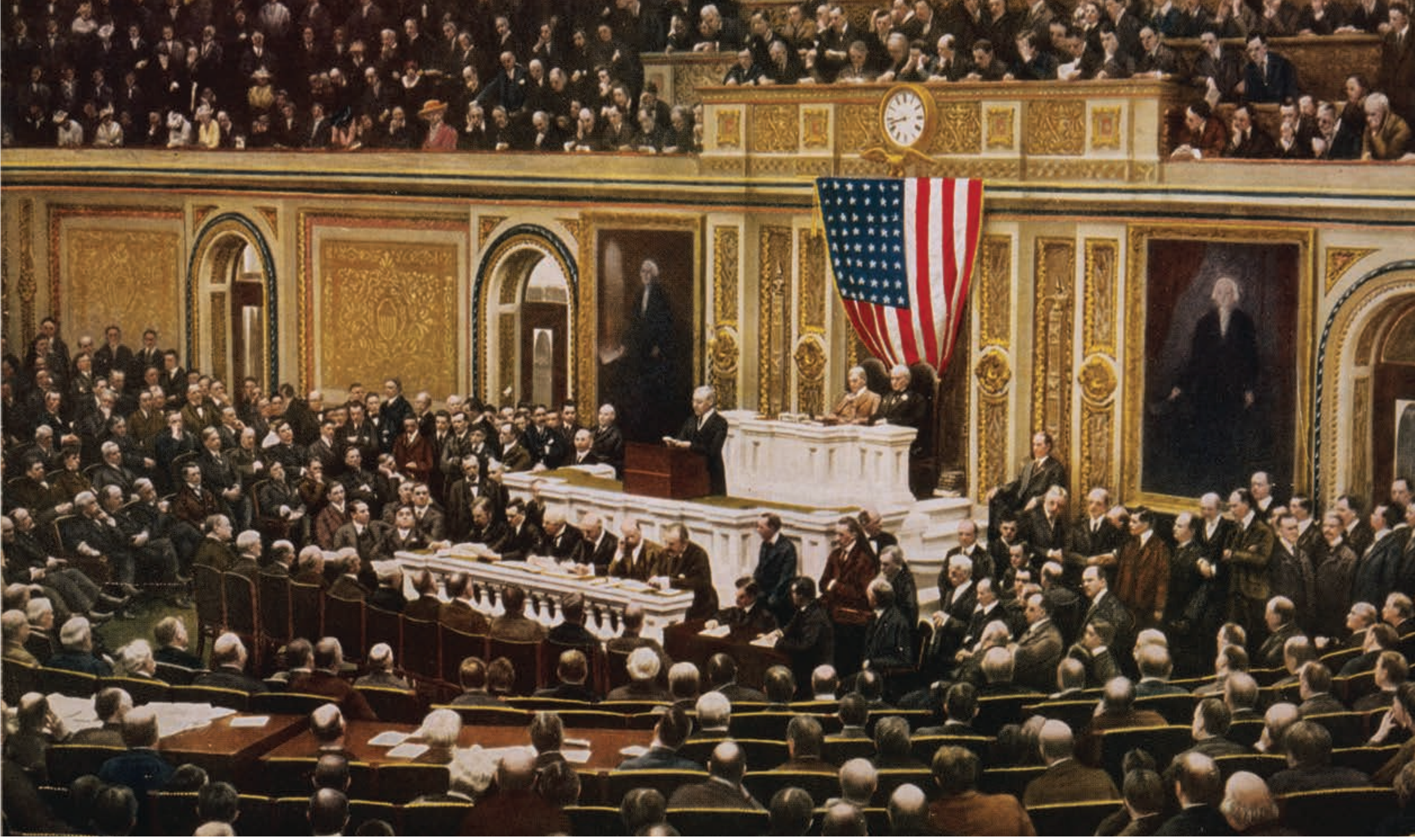
In their invasion of Ukraine in February 2022, the Russians mobilized between 150,000 and 190,000 men.[12] They faced initially a 250,000-man Ukrainian army.[13] The Russians employed seven combined arms armies and elements of two others plus one guards tank army. They also deployed airborne, naval infantry, and Spetsnaz light infantry around Ukraine's borders.[14] The Russians not only had numerically inadequate forces to defeat and effectively control Ukraine—a country covering some 233,000 square miles (600,000 square kilometers) and with a population of about 41 million (in January 2022)—but they also grossly underestimated the Ukrainian ability to use skillfully their smaller but better trained and highly motivated forces both in defense and on offense.

One of the most important factors in determining a military-strategic objective is to have a realistic assessment of the *duration of a pending war*. Ideally, this should be based on a consensus between military leaders and civilian security officials. Yet sometimes a single powerful ruler, as was Adolf Hitler or Joseph Stalin, and his inner circle might arbitrarily decide the duration of a pending war. Major pitfalls are the gross underestimation of the enemy's capabilities and the will to fight. In his decision to invade Soviet Russia, Hitler expected that the entire campaign would not last more than 8 to 12 weeks.[15] The German high command shared these views. So it was not surprising that for the Germans, the Soviet abundance of natural resources, number of divisions, tanks, aircraft, and vast distances could be safely disregarded. Although the German generals might not have had full knowledge of the Soviet capabilities, they still should have known the limitations of their own forces. To achieve a decisive victory, they needed a much larger force in their Eastern Campaign. Yet the Germans started it with a force slightly larger than in their campaign in the West in 1940, especially in terms of numbers of panzers and aircraft.[16]

Prior to the invasion of Ukraine on February 24, 2022, Russian leadership made an incorrect assumption about the duration of the war. Russian intelligence assumed that there would be no serious Ukrainian resistance, that some units with a Russian-speaking population would refuse to fight, and that the Russian population in the eastern provinces would welcome Russian troops as liberators.[17] A captured Russian document in March 2022 stated that by the 10th day of the invasion, the Russian forces would transit to stabilization operations. They would "proceed to the blocking and destruction of individual scattered units of the [enemy] Armed Forces and the remnants of the nationalist resistance units." The Russian "special services" would be used for establishing occupation administration on the "liberated" territories.[18]

In other cases, military leadership was correct in its assessment about the duration of the war but decided to open hostilities because of the anticipated negative trend in the correlation of forces. In 1941, most of the Japanese high command assumed that a war with the Western powers would be long. Yet the longer Japan waited to initiate a war against the United States, the dimmer the prospects for success because of accelerated U.S. rearmament. This was especially the case in naval strength. In 1941, the Imperial Japanese Navy had some 70 percent of the tonnage of the U.S. Navy. However, the U.S. plan for a two-ocean Navy in July 1940 called for a 70 percent increase in U.S. naval tonnage. By 1943, the ratio for Imperial Japanese Navy to U.S. Navy would be reduced to 50 percent, and in 1944 to 30 percent. The Japanese were not realistic in their assumptions that by quickly capturing the central and southwestern Pacific and then fortifying these positions, they would force the Americans into a protracted island-by-island slog. They also erroneously believed that the cost of the struggle would be beyond America's willingness to pay.[19]

Optimally, one should possess accurate, timely, and relevant intelligence on the enemy's military-strategic capabilities. This is often not possible because



President Woodrow Wilson asks Congress to declare war on Germany, April 2, 1917 (Library of Congress, colorized)

there are so many variables involved in intelligence assessment—and intelligence is rarely perfect. Both accurate and inaccurate, and sometimes wide of the mark or misleading, statements are part of the same strategic assessment. Exaggeration of friendly capabilities and underestimation of those of the enemy are common. The lack of good intelligence is often the reason for underestimating the enemy's military capabilities, as the example of the Russian military in the Far East in 1904 illustrates. Russian commanders had only the barest of information concerning Japan. They had inaccurate numbers of divisions and capital ship dispositions.[20] At the same time, Tsar Nicholas II and his inner circle had a strong belief that Japan would not dare take up arms against the all-powerful Russian army and navy. One exception was General Aleksey P. Kuropatkin, minister of war, who did an inspection tour of East Asia from May to July in 1903. He reported that Russian forces were in a good state but that the Japanese army was equally strong. Kuropatkin argued that war with Japan should be avoided at all costs. At an important meeting in Port Arthur in early July 1903, Kuropatkin's views were endorsed. However, the war with Japan became inevitable after early August 1903, when Vice Admiral Yevgeni I. Alekseyev was appointed as a viceroy in the Far East with headquarters in Port Arthur. He maintained hard and unyielding policies during negotiations with Japan.[21]

During planning for the invasion of Soviet Russia, the Germans greatly underestimated the numerical strength of the Red Army in western Russia. The Supreme Command of the Army (Oberkommando des Heeres, or OKH)'s intelligence department estimated that the Soviets deployed 147 divisions plus 39 to 40 independent brigades. However, the Soviets deployed in four western military districts 180 divisions and 44 to 45 independent brigades.[22] In January 1941, the OKH's intelligence estimated the Red Army's strength as 150 rifle divisions (including 15 motorized and 32 cavalry divisions and 36 motorized brigades).[23] After mobilization, the Soviets would have a total of 209 divisions (107 rifle divisions in the first wave, 77 rifle divisions in the second wave, and 25 rifle divisions in the third wave).[24]

In the later phase of planning, the OKH's intelligence estimated that the Red Army deployed in western Russia 213 divisions (including 25 divisions against Finland and in the Transcaucasus). In the area between the Baltic and the Black seas, 204 divisions (133 rifle divisions, 24 cavalry divisions, 10 tank divisions, and 37 motorized divisions) were deployed. No estimates were made for the second wave of the Red Army's strength after mobilization.[25] The OKH's intelligence believed that from the Asian theater the Red Army could bring in 38 divisions (25 rifle and 8 cavalry divisions and 5 motorized brigades) of the third wave. Some of them could be used against the Germans after the nonaggression pact with Japan was signed in April 1941.[26] However, the Soviets had 303 divisions in June 1941, or 93 more than the Germans believed. The Germans estimated that the Soviets had some 10,000 tanks, but the real number was 23,100; the number of aircraft was

Brigadier General Courtney Whitney; General Douglas MacArthur, Commander-in-Chief, United Nations Command; and Major General Edward M. Almond observe shelling of Inchon from USS *Mount McKinley*, September 15, 1950 (U.S. Army)

estimated as 6,000 (5,500 frontline), of which some 3,300 were deployed in western Russia. However, the Soviets had some 20,000 aircraft in their inventory, including 9,300 in western Russia.[27]

Another problem is the tendency to focus on the enemy's intentions instead of its capabilities. This has probably been the cause of more major military failures than any other intelligence deficiency. It is common to make an error in estimating the enemy's intentions because of one's inability to think from the enemy's frame of reference. The British made such an error in January 1940 regarding possible German landings in Norway. They firmly believed that the Germans would not intervene in Scandinavia if their iron ore imports were not endangered or if the Allies did not establish a naval base on the Norwegian coast.[28]

In the absence of reliable information, military commanders and their staffs must make certain strategic assumptions that might be true or only partially true, or even entirely false. Realistic military-strategic assumptions have a critical role in determining military-strategic objectives. Yet this is often not the case for a variety of reasons, such as wrong perceptions, racial prejudice, a sense of cultural superiority, or relying on suspect historical precedents. In 1941, the Germans believed that the Soviets had a limited reconstitution and mobilization capacity and that they would get little support from the Western Allies.[29] The German perception of the poor state of the Soviet military was based on its experiences with the Russians in World War I and the Freikorps (Free Corps) fighting in the Baltics in 1919. The Germans were also influenced by the information the Japanese shared about interrogations of a high-ranking Soviet defector (General Genrikh S. Lyushkov, the Soviet secret service chief in the Far Eastern Army, who defected to the Japanese in June 1938).[30] The German military was aware of Stalin's purges of the Soviet officer corps in 1937–1938, and that led them (not unreasonably) to believe that the Soviet military was weak. The Germans also assumed that a surprise attack would lead to a swift victory. This wishful thinking led to a lack of planning for fighting in the Russian winter and for ignoring German logistical shortfalls.[31] For his part, Stalin was well informed about the scale of the German buildup in the east but made a fatal error in believing that Hitler did not plan to attack.[32]

In preparing for their invasion of Ukraine, Russian leaders made several false political and military assumptions. The Central Intelligence Agency director testified in early March 2022 that Vladimir Putin "was confident that he had modernized his military, and they were capable of quick and decisive victory at minimal cost."[33] These assumptions possibly determined and imposed unrealistic objectives and timetables on the Russian military. The Russians also vastly underestimated the quality, morale, and determination of Ukraine's armed forces—a clear evidence of hubris.[34]

The Process

Ideally, the process of converting a political objective to a military-strategic objective should consist of several mutually related and consecutive steps. It should result in determining the main and alternative military- or theater-strategic objectives. In a war, one's main strategic objective should not be too obvious. Liddell Hart observed that an alternative objective would provide "the opportunity of gaining an objective, whereas a single objective, unless the enemy is helplessly inferior, means the certainty that you will not gain it—once the enemy is no longer uncertain as to your aim."[35]

The process should start by conducting a strategic estimate in a pending theater of war (see figure 2). That estimate is normally a part of the overall strategic estimate (that encompasses not only military but also nonmilitary aspects of a strategic situation). Normally, a military-strategic estimate should encompass a thorough assessment of friendly, enemy, and neutral forces, plus the effect of the physical environment (terrain, oceanography, climate/weather) on their employment in combat. For both friendly and enemy forces, their strengths and weaknesses/vulnerabilities should be identified and evaluated. Special attention should be given to intangible elements of both friendly and enemy forces.

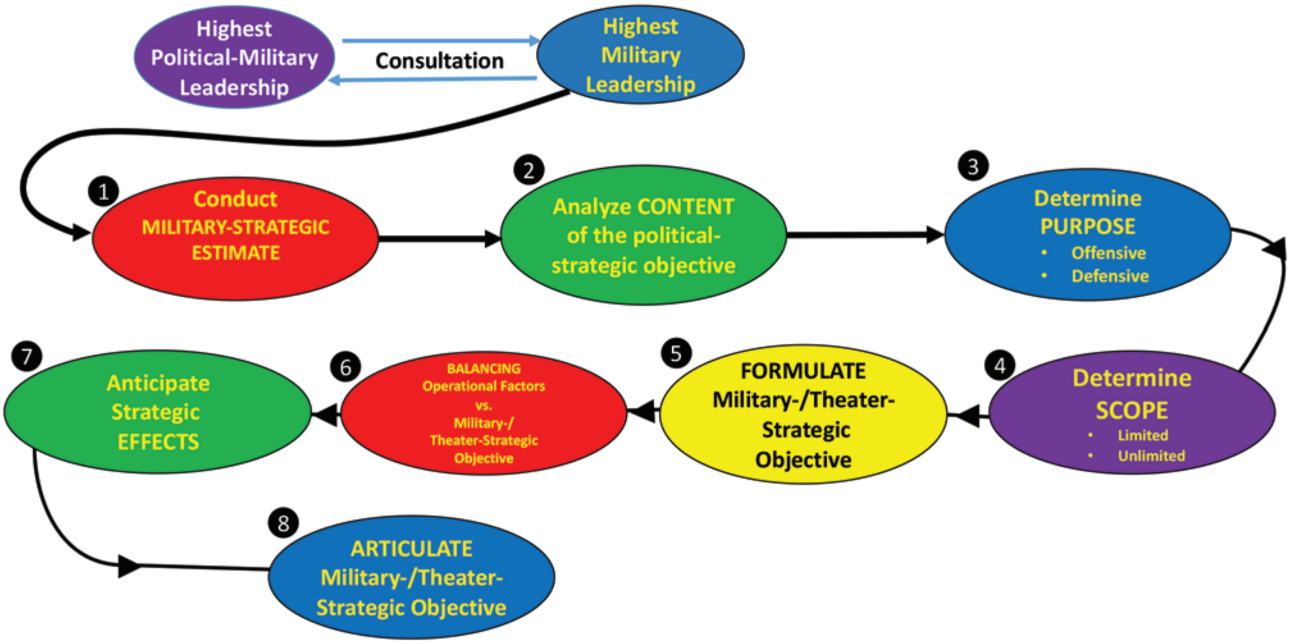
For converting a military-strategic objective to theater-strategic objectives, an estimate of the military situation should be conducted for a given theater of operations. Then each theater-strategic objective should be in consonance with a given political objective in the respective theater of operations. The military- or theater-strategic estimate should end with conclusions and recommendations (or lines of effort) for essential aspects of the military-strategic situation.

Military-strategic leadership must carefully analyze the content of political objectives issued by the highest politico-military leadership. The primary purpose is to identify those parts of political objectives that require the use of military force. Normally, one's sources of military power would be used to obtain political or ideological dominance of a certain area, overthrow the enemy regime, change the enemy's social system, or impose control of the enemy's economic resources.

In the next step, the main purpose of a given political objective should be evaluated. Generally, an offensive political objective would require the accomplishment of offensive military-strategic objectives. For their "first operational stage of the war" in 1941–1942, the Japanese selected offensive military strategic objectives: to gain mastery of the Far East area by destroying U.S. power in the western Pacific and British forces in the Far Eastern waters and cutting their respective sea communications with these areas and land communications from India to China (the Burma Road).[36] In November 1941, the central Japanese army-navy agreement specified that the war objectives were "reduction of foundation of U.S., British, and Dutch power in Eastern Asia, and occupation of Southern Areas."[37] The U.S. Joint Staff directive of July 2, 1942, to General Douglas MacArthur, Supreme Commander, Southwest Pacific Area, stated that his ultimate (theater-strategic) objective was "seizure and occupation of New Britain–New Ireland–New Guinea area."[38]

Sometimes political-strategic objectives were offensive, but they were not supported by offensive military-strategic objectives. Russia's political objectives in its war against Japan in 1904–1905 were clear: maintain control over Manchuria and decisively repel Japanese advances. Yet the Russian military-strategic objective was defensive: retain control of the positions they already held in Port

Figure 2. Steps for Converting a Political Objective to a Military-/Theater-Strategic Objective


Highest Political-Military Leadership
Consultation
Highest Military Leadership
1
Conduct MILITARY-STRATEGIC ESTIMATE
2
Analyze CONTENT of the political-strategic objective
3
Determine PURPOSE
• Offensive
• Defensive
4
Determine SCOPE
• Limited
• Unlimited
5
FORMULATE Military-/Theater-Strategic Objective
6
BALANCING Operational Factors vs. Military-/Theater-Strategic Objective
7
Anticipate Strategic EFFECTS
8
ARTICULATE Military-/Theater-Strategic Objective

Arthur, the Trans-Siberian Railway, Vladivostok, and other concessions on the Yalu River.[39] Russia's proper military-strategic objectives were destruction of the Japanese forces in Manchuria and obtaining/maintaining control of the Yellow Sea and the Sea of Japan.

Defensive military-strategic objectives are usually selected by the side on the strategic defensive. They could sometimes be combined with some preparatory measures to go on the offensive. The Combined Chiefs of Staffs directive to Admiral Chester W. Nimitz, Commander in Chief, Pacific Ocean Areas/U.S. Pacific Fleet, on March 30, 1942, stated the following objectives:

a) Hold the island positions between the United States and the Southwest Pacific Area necessary for the security of the line of communications between those regions; and for supporting naval, air and amphibious operations against Japanese forces; (b) Support the operations of the forces in the Southwest Pacific Area; (c) Contain Japanese forces within the Pacific Theater; (d) Support the defense of the continent of North America; (e) Protect the essential sea and air communications; and (f) Prepare for the execution of major amphibious offensives against positions held by Japan, the initial offensives to be launched from the South Pacific Area and Southwest Pacific Area.[40]

Sometimes, the weaker side had a defensive political objective, but the only way of accomplishing it was by going strategically on the offensive. In the American Civil War (1861–1865), the Confederate states had a defensive political-strategic objective: force the Union to recognize Confederate independence. However, this could be accomplished only by selecting an offensive military-strategic objective.[41]

Like a political objective, a military-/theater-strategic objective may be unlimited or limited. An unlimited objective would be selected if the political objective is to overthrow the enemy's government and/or social system or capture a major part of the enemy's territory. In a case of war between two strong opponents, accomplishing an unlimited military strategic objective would usually result in a long war requiring maximum exertion of all spiritual and material resources of a nation or an alliance/coalition, as the war on the Eastern Front in 1941–1945 illustrated. In other cases, a much stronger side might accomplish its offensive and unlimited political- and military-strategic objectives relatively quickly, as the German invasion of Poland in September 1939, Norway in April 1940, and Yugoslavia and Greece in April 1941 demonstrated.

In its invasion of Ukraine, Russia initially selected offensive and unlimited political and military-strategic objectives. Putin expected to capture Ukraine's capital Kyiv quickly and install a compliant government. He reportedly believed that the Ukrainian military would be ineffective and that the Ukrainian political leadership could be easily replaced.[42] Rapid takeover of Ukraine would present the West with a fait accompli.[43]

In a war fought for limited political objectives, a military-/theater-strategic objective would also usually be limited. One normally does not risk all for limited political objectives, nor does one commit all his sources of power in such a war.[44] Accomplishing a limited military-/theater-strategic objective would require low to modest use of military power, efforts, and time. A state might not need to pursue an unlimited military-strategic objective by trying to destroy the enemy's forces and seek their surrender. Liddell Hart wrote that a state seeking not conquest, but the maintenance of its security would accomplish its military-strategic objective if the threat is removed and "if the enemy is led to abandon his purpose."[45] Or it "may desire to wait until the balance of forces can be changed by the intervention of allies or by referring forces from another theater. It may desire to wait, or even to limit the military effort permanently, while naval or economic action decides the issue."[46]

The Gulf War of 1990–1991 had limited political- and military-strategic objectives. The U.S.-led coalition never intended to defeat the Iraqi armed forces as a whole and occupy the entire Iraqi territory. The coalition objectives called for immediate, complete, and unconditional withdrawal of all Iraqi forces from Kuwait, restoration of the legitimate Kuwaiti government, the security and stability of Saudi Arabia and the Persian Gulf, and the safety and protection of American citizens abroad.[47] The United States aimed to remove Saddam Hussein by his domestic opposition but without endangering Iraqi territorial integrity. The coalition did not intend to defeat Iraq so completely that the ensuing power vacuum would be exploited by Iran and spark further turmoil there.[48] The United States was unwilling to pursue its objectives directly and did not intend to be involved in the nation-building and humanitarian relief that would surely follow the overthrow of the Iraqi regime. At the time, a serious disconnect existed between the more ambitious ends and modest means to be used by the United States and its coalition partners. Hence, it was not surprising that the termination of the Gulf War was not only confused and ambiguous but also had unintended and adverse consequences for U.S. national interests.[49]

The geographical separation of centers of power of the opponents plays an important role in a war for limited military-/theater-strategic objectives. This is especially the case when there is a lack of an overland link between the two main belligerents due to an ocean or neutral states or if the land area is so large as to make it difficult or impossible for either belligerent to exert its full strength against the other.[50] The Russo-Japanese War of 1904–1905 was a war with limited political- and military-strategic objectives for both sides. Both Russia and Japan disputed control of the area, which did not belong to either of them. Japan was unable to completely defeat Russia, but that was also unnecessary. This was also the case for Russia. Neither Japan nor Russia wanted to fight to the end. Thus, they were unwilling to commit their utmost efforts and sacrifices, which might have led to a complete exhaustion.[51] The Russian tsar and his inner circle argued for land acquisition, while Russian Prime Minister Sergei Witte was more interested

B-1B Lancer is refueled by KC-135 Stratotanker, February 26, 2011, above Iraq, in support of Operation *New Dawn* (U.S. Air Force/Adrian Cadiz)

in commercial expansion in the Far East.[52] Japan felt humiliated and double-crossed by the Russian acquisition of Port Arthur from 1895 onward. It was also staunchly opposed to growing Russian influence in Manchuria. By going to war, Japan claimed that its aim was to "liberate" Manchuria from the Russian grasp.[53] The Japanese military objectives were in consonance with the political-strategic objectives. Specifically, the Japanese aimed to capture the Korean Peninsula and then destroy the Russian army in Manchuria. Preconditions for this were to obtain control of the Yellow Sea and ensure security of land and sea communications between Korea and Manchuria.[54]

A stronger side might be forced to change its military-strategic objective from unlimited to limited because of a series of military setbacks or defeats in the field. By early April 2022, for instance, the Russian offensive in Ukraine stalled. The Russians were unable to capture Kyiv or Kharkiv, so Russian forces began to withdraw from the vicinity of Kyiv and were redeployed to the self-declared Donetsk and Luhansk people's republics. Once the Russians realized that their political objectives could not be achieved, they for the time being reduced both their political- and their military-strategic objectives. This was formally announced on April 26, 2022. Afterward, the Russians launched an offensive to fully occupy the Donetsk and Luhansk republics and strengthen their control in southern Ukraine.[55] That offensive failed to achieve its stated objectives. By December 30, 2022, the Russian forces were generally on the defensive except for some limited ground assaults against selected positions in the eastern part of Kharkiv, the Donetsk and Luhansk republics, and the southern area.[56]

In contrast, Ukraine's initial political- and military-strategic objectives were defensive and limited to preserving territorial integrity, protecting Kyiv and major cities, and surviving until Western support arrived.[57] Because of battlefield successes, the Ukrainian military-strategic objectives were changed in the spring of 2022. The Ukrainian forces went on the offensive and recaptured a relatively large part of eastern Ukraine, including the city of Kherson in southern Ukraine, in November 2022. By November 12, the Ukrainians liberated 28,742 square miles of their sovereign territory (the Russians still control 17,165 square miles).[58] Their political objective remains essentially defensive, but the military-strategic objectives were expanded to recovery of the territories lost to Russia in 2014 and 2022.[59]

Sometimes a side on a strategic defensive might go on the offensive but will select a limited military-/theater-strategic objective, as the United Nations (UN) forces in Korea in the summer of 1950 illustrate. However, the success of a counteroffensive might lead political and military leadership to change the military-strategic objective from limited to unlimited. After the UN amphibious landing in Inchon on September 15, 1950, the Joint Chiefs of Staff directed General MacArthur on September 27, 1950:

Your military objective is the destruction of the North Korean armed forces. In attaining this objective, you are authorized to conduct military operations, including

Paul D. Wolfowitz, Under Secretary of Defense for Policy, right, takes notes while General Colin Powell, Chairman of the Joint Chiefs of Staff; and General Norman Schwarzkopf, Commander-in-Chief, U.S. Central Command, take part in press conference held by U.S. and Saudi Arabian officials during Operation *Desert Storm*, circa February 1991 (DOD/Susan Carl)

amphibious and airborne landings or ground operations north of the 38th parallel in Korea provided that at the time of such operations there has been no entry into North Korea by major Soviet or Chinese Communist forces, no announcement of intended entry, nor a threat to counter our operations militarily in North Korea.[60]

In the process of formulating a military- or theater-strategic objective, military leaders and planners should reevaluate the validity of the preceding steps regarding the purpose (offensive or defensive) and scope and intensity of efforts (limited or unlimited) of the selected objectives. Another critical part is to identify the type of action and desired damage to inflict on enemy forces. Clearly, actions intended to accomplish an offensive objective differ significantly from those aimed at achieving a defensive objective. An offensive military- or theater-strategic objective is accomplished by the destruction, annihilation, or neutralization of the major part of the enemy's armed forces. The enemy is destroyed when the core of his forces suffers such losses that he cannot continue the fight.[61] The enemy is annihilated when he is left with no sources of power to offer any serious resistance. Neutralization means that the enemy is rendered ineffective and cannot prevent friendly forces from accomplishing their assigned objective.[62] Defensive military- or theater-strategic objectives are expressed in terms of containing, defending, delaying, preventing, retaining, or denying control regarding the enemy's forces or a given geostrategic position/territory or sea/ocean area.

After a military-/theater-strategic objective is formulated, the next step is to balance it with the operational factors of space, time, and force (see figure 3).[63] In this process, all considerations should start with quantifiable factors—that is, space and time.[64] The factor of time is more dynamic and changeable than the factor of space. The key elements of the factor of space related to military-/theater-strategic objectives are geostrategic positions, the country or territory's size or shape, strategic distances, the country's capital and other large urban centers, and economically important areas. Strategically important elements of the factors of time include anticipated duration of a war, time for preparing for a war, time for opening the hostilities, strategic warning and reaction times, and time required for strategic deployment of one's forces. The factors of space and time can be evaluated with a relatively high degree of precision.

In contrast, the factor of force is extremely difficult to assess because of the presence of not only tangible (or physical) but also numerous intangible (or abstract) elements. For military-/theater-strategic objectives, the most important tangible elements of the factor of force are the overall size/composition of the armed forces and individual services prior to the hostilities and their anticipated expansion in a war, size/composition of strategic reserves and force reinforcements, overall number/quality of the main weapons, firepower, strategic mobility, and so forth. Intangible elements of the factor of force pertain for the most part to the human factor. The most critical of these elements related to the military-/theater-strategic objective are the national will to fight, cohesion of the alliance/coalition, quality of strategic leadership, soundness of joint/combined doctrine, morale/discipline, and state of combat readiness of the armed forces and individual services. Such elements cannot be expressed in quantifiable terms but only in very broad terms: low, medium, high, or excellent, sound, unsound.

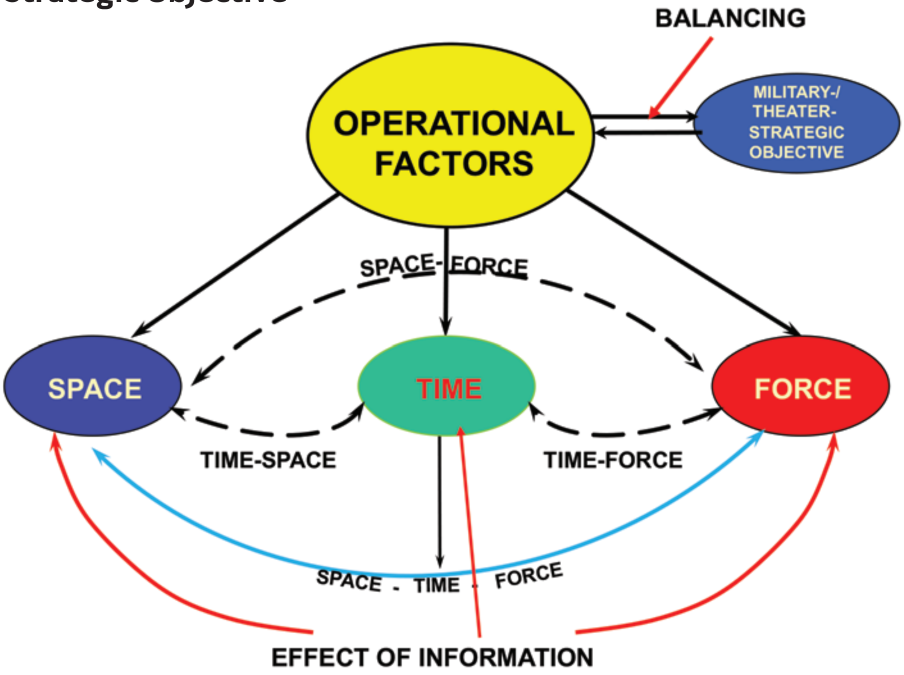
In addition to these three traditional factors, information has emerged as a possible fourth operational factor. However, despite all the technical advances, the inherent characteristics of information have not been changed. One cannot control or anticipate volume, accuracy, timeliness, and relevance of information received. Unlike traditional operational factors, information is not meaningfully definable. Hence, it cannot be balanced with a given military objective. Yet strategic leaders should make all efforts to evaluate the effect of information on the operational factors of space, time, and force individually.

A serious disconnect between the military-/theater-strategic objective and any of the three operational factors must be somehow resolved; otherwise, there would be a real danger of suffering a major setback or even failing to accomplish the objective. The resolution of this problem might require reducing the space for the employment of friendly forces, dividing space into several segments to offer better opportunities for advance or defense, increasing numerical superiority, assigning more lethal or mobile forces, extending the timeline, using strategic deception and/or surprise, and so forth. If a disconnect cannot be adequately resolved, then the military-/theater-strategic objectives must be modifed, altered, or even abandoned. The process of balancing is largely an art, not a science. Hence, a sound solution is heavily dependent on the experience, judgment, and creativity of the military strategic leadership.

Military-strategic leaders must also give some thought to anticipating possible strategic effects after the objective is accomplished. Much depends on their knowledge and understanding of the enemy and all aspects of both the military and the nonmilitary situation. These effects of accomplishing a military-/theater-strategic objective can be positive (desired) or negative (undesired). They can be military or nonmilitary and tangible or intangible (or both). In most cases, the type of effects and their strength and duration cannot be accurately predicted, much less precisely calculated. The effect of accomplishing or failing to achieve the military-/theater-strategic objective might not be immediately recognized by the enemy and friendly or neutral sides; it might be some time before the effects of one's actions are felt or fully understood. These effects might sometimes lead to dramatic changes in the diplomatic, political, economic, social, religious, informational, psychological, and other aspects of the situation in each theater.

National and military strategic leaders should also fully consider political, diplomatic, economic, financial, ethnic, religious, and other nonmilitary aspects of the strategic situation. Foreign policy or domestic political considerations might dictate whether a certain objective should be selected for a military action. This is especially the case in the initial phase of a war. In drafting his plans for the possible war with France and Russia, Field Marshal Alfred von Schlieffen, Chief of the German General Staff (1891–1905), believed that in the coming war, Germany must unconditionally go on the offensive and, therefore, invade France. Schlieffen did not consider the possibility of going on the offensive against Russia in case of war in the Balkans and remaining on the defensive against France and not violating Belgian neutrality—thereby possibly keeping Britain out of the war. His successor, Field Marshal Helmuth von Moltke, Jr., directed in a memorandum in 1913 that all planning for a great offensive against Russia be stopped because he was concerned that, in case of war, the existence of such a deployment plan could lead to confusion for subordinate commands. The German government was also fully informed that the General Staff had stopped all planning against Russia. In the same memo, Moltke noted (accurately) that the violation of Belgian neutrality might force England to enter the war on the side of Germany's enemies. Yet instead of canceling plans to invade Belgium, Moltke decided just the opposite—making the right flank as strong as possible and invading France through Belgium.[65]

Figure 3. Operational Factors Vs. the Military-/Theater Strategic Objective



In deciding to go to a war of choice against a weaker opponent, it is necessary to realistically assess the possibility that such a course of action might lead to intervention of other and stronger powers. The Austro-Hungarian political leaders made a fatal mistake in declaring war on Serbia on July 28, 1914. This action led to a chain of events that eventually involved all major European powers in a world war.

The faulty assumptions about possible reaction of the potential enemies often result in escalation and a much larger war, as the example of Nazi Germany in its unprovoked attack on Poland on September 1, 1939, illustrates. Hitler was confident that the Western powers (Great Britain and France) would not intervene. Hitler stated, "I have met the umbrella men, Chamberlain and Daladier, at Munich and got to know them." Hitler assured his generals when they expressed doubts on the matter that "they can never stop me from solving the Polish question. The coffee sippers in London and Paris will stay still this time too." Hitler's conviction that the Western powers would not intervene was initially strengthened because the powers did not issue an immediate ultimatum.[66] Great Britain and France declared war on Germany on September 3, 1939. The rest is history.

Putin and his inner circle and intelligence agencies clearly failed to properly assess the strategic effects of their invasion of Ukraine in February 2022. This event led to radical changes in the security situation not only in Europe but globally as well. The United States, the European Union, and some other Western countries imposed massive and unprecedented economic sanctions against Russia. It greatly strengthened the North Atlantic Treaty Organization. It led two staunchly neutral countries, Sweden and Finland, to ask for membership in the Alliance. Russia was forced to increase its dependence on China for the export of gas and oil. Its geopolitical situation is much more unfavorable than it was prior to February 2022. The consequences of invasion of Ukraine were certainly not what Putin envisaged.[67]

A military-/theater-strategic objective should be articulated clearly, concisely, and unambiguously. A great example of a clearly stated military strategic objective was the February 12, 1944, directive by the Combined Chiefs of Staff to General Dwight Eisenhower, Supreme Commander of the Allied Expeditionary Forces, for the invasion of the European continent. It stated that Eisenhower's task was to

> *enter the continent of Europe, and, in conjunction with the other United Nations, undertake operations aimed at the heart of Germany and the destruction of her armed forces. The date for entering the Continent is the month of May 1944. After adequate* [English Channel] *ports have been secured, exploitation will be directed to securing an*

Eisenhower meets with Company E, 502nd Parachute Infantry Regiment (Strike), of 101st Airborne Division, at Royal Air Force Greenham Common, England, about 8:30 p.m., on June 5, 1944, and speaks to, among others, Wallace C. Strobel (on his 22nd birthday, wearing number 23, which designated plane 23, on which he was jumpmaster) (U.S. Army)

President of Ukraine Volodymyr Zelensky reviews plans during working trip to Kharkiv region, November 30, 2023 (President of Ukraine)

area that will facilitate both ground and air operations against the enemy.[68]

In the Korean War (1950–1953), U.S. and UN objectives were unclear. The UN Resolution of June 27, 1950, called for repelling the Democratic People's Republic of Korea attack and restoring "peace and security." Repelling an attack implied restoring the border between North and South Korea on the 38th parallel north, but restoring peace and security was not defined.[69] Another cause of confusion was that the Joint Chiefs of Staff directed MacArthur to submit plans for the occupation of North Korea. The Joint Chiefs of Staff thought in terms of a contingency plan, but MacArthur understood it as a mission.[70]

Ideally, a military-/theater-strategic objective should not be grouped together with political-strategic objectives. Clarity and simplicity are grossly violated by adding purely operational objectives, or even worse, routine military activities, as the Pentagon's public statement on the objectives for the invasion of Iraq in March 2003 illustrate.[71]

The process of converting political- to military-strategic objectives is the first and most critical step prior to the actual employment of one's armed forces in war. The personality traits of the highest military leaders and their experience and judgment have extraordinary importance in the entire process. Military-strategic leaders should inform their political counterparts about the purpose and scope of the military- or theater-strategic objective; otherwise, there is a danger that these objectives will not be aligned with the aims of policy. At the same time, political leaders should make sure that sufficient forces are available to accomplish the military- or theater-strategic objective. Every effort should be made to avoid such common mistakes as overestimating one's own military capabilities and underestimating the enemy's. The assessment of the military capabilities will be grossly deficient if the focus is primarily or, even worse, exclusively on materiel. The strengths and weaknesses of human factors must be an integral part of any analysis of both friendly and enemy military capabilities. **JFQ**

Notes

[1] Cited in Joel E. Hamby, "Striking the Balance," *Armed Forces & Society* 30, no. 3 (Spring 2004), 334.

[2] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 81.

[3] B.H. Liddell Hart, *Strategy*, 2nd rev. ed. (New York: Frederick A. Praeger Publishers, 1967), 352.

[4] "Joint Chiefs of Staff Memorandum: Strategic Plan for the Defeat of Japan. Approved by the Combined Chiefs of Staff, 19 May 1943" (JXS 287/1 and CCS 220), in Louis Morton, *United States Army in World War II. The War in the Pacific. Strategy and Command: The First Two Years* (Washington, DC: U.S. Army Center of Military History, 1989), 644, https://history.army.mil/html/books/005/5-1/CMH_Pub_5-1.pdf.

[5] Friedrich von Bernhardi, *On War of To-Day*, vol. 1, *Principles and Elements of Modern War*, trans. Karl von Donat (New York: Dodd, Mead & Company, 1914), 94.

[6] Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Vintage Books, 1991), 201.

[7] Alfred Philippi and Ferdinand Heim, *Der Feldzug gegen Sowjetrussland, 1941–1945* (Stuttgart: W. Kohlhammer Verlag, 1962), 36.

[8] George E. Blau, *The German Campaign in Russia: Planning and Operations (1940–1942)*, Army Pamphlet No. 20-261a (Washington, DC: Department of the Army, March 1955), 14.

[9] Intended for fighting insurgents in the rear of the field armies and conducting punitive actions against civilian populations.

[10] Philippi and Heim, *Der Feldzug gegen Sowjetrussland, 1941–1945*, 37.

[11] Blau, *The German Campaign in Russia*, 15.

[12] Andrew S. Bowen, *Russia's War in Ukraine: Military and Intelligence Aspects*, R47068 (Washington, DC: Congressional Research Service, September 14, 2023), 1, https://crsreports.congress.gov/product/pdf/R/R47068.

[13] Denys Davydenko et al., "Lessons for the West: Russia's Military Failures in Ukraine," European Council on Foreign Relations, August 11, 2022, 1, https://ecfr.eu/article/lessons-for-the-west-russias-military-failures-in-ukraine/.

[14] Bowen, *Russia's War in Ukraine*, 2.

[15] Charles T. Crenshaw, *Distinctions Between Tactical and Operational Levels of War: Are Some More Important Than Others?* (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, May 1986), 19.

[16] Evan Mawdsley, *Thunder in the East: The*

Nazi-Soviet War, 1941–1945 (London: Hodder Arnold, 2007), 41–42.

[17] Ioannis E. Kotoulas and Wolfgang Pusztai, *Geopolitics of the War in Ukraine*, Report No. 4 (Athens, Greece: Foreign Affairs Institute, June 2022), 28.

[18] Mykhaylo Zabrodskyi et al., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* (London: Royal United Services Institute for Defence and Security Studies, 2022), 9, https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

[19] Jeffrey Record, *Japan's Decision for War in 1941: Some Enduring Lessons* (Carlisle, PA: U.S. Army War College Press, February 2009), 24–25, 27.

[20] Hamby, "Striking the Balance," 337.

[21] Ian Nish, "The Russo-Japanese War: Planning, Performance and Peace-Making," in *Der Russisch-Japanische Krieg (1904/05)*, ed. Josef Kreiner (Bonn: Bonn University Press, 2005), 13.

[22] Mawdsley, *Thunder in the East*, 42.

[23] Walter Post, *Unternehmen Barbarossa. Deutsche und sowjetische Angriffspläne 1940/41* (Berlin: Verlag E.S. Mittler & Sohn GmbH, 1995), 228.

[24] Ibid.

[25] Philippi and Heim, *Der Feldzug gegen Sowjetrussland, 1941–1945*, 36.

[26] Ibid.

[27] Mawdsley, *Thunder in the East*, 42.

[28] Olivier Desarzens, *Nachrichtendienstliche Aspekte der "Weserübung" 1940* (Osnabrück: Biblio Verlag, 1988), 79, 89, 91.

[29] David C. Gompert, Hans Binnendijk, and Bonny Lin, *Blinders, Blunders, and Wars: What America and China Can Learn* (Santa Monica, CA: RAND, 2014), 89.

[30] Post, *Unternehmen Barbarossa*, 225.

[31] Gompert, Binnendijk, and Lin, *Blinders, Blunders, and Wars*, 89.

[32] Mawdsley, *Thunder in the East*, 34.

[33] Bowen, *Russia's War in Ukraine*, 11.

[34] Matthew Sussex, "Putin's War in Ukraine: Missteps, Prospects, and Implications," *Australian Journal of Defence and Strategic Studies* 4, no. 1 (July 2022), 93.

[35] Hart, *Strategy*, 348–349.

[36] Ministry of Defence (Navy), *War With Japan*, vol. 1, *Background to the War* (London: His Majesty's Stationery Office, 1995), 84.

[37] Ibid., 134–135.

[38] "Appendix E. Joint Directive for Offensive Operations in the Southwest Pacific Area Agreed Upon by the United States Chiefs of Staff, 2 July 1942," in Morton, *Strategy and Command*, 619.

[39] Hamby, "Striking the Balance," 336.

[40] Morton, *Strategy and Command*, 617–618.

[41] Günther Korten, *Erfahrungen über Wehrmachtsführung aus dem amerikanischen Sezessionkrieg*, lecture at the Kriegsakademie, March 1936, RW 13/v. 34, Bundesarchiv-Militärarchiv, Freiburg, i. Br., 13.

[42] Cited in Bowen, *Russia's War in Ukraine*, 11.

[43] Rob Johnson, "Dysfunctional Warfare: The Russian Invasion of Ukraine 2022," *Parameters* 52, no. 2 (Summer 2022), 5, 8, https://press.armywarcollege.edu/parameters/vol52/iss2/8/.

[44] Bruce B.G. Clarke, *Conflict Termination: A Rational Model* (Carlisle Barracks, PA: Strategic Studies Institute, May 1992), 11.

[45] Hart, *Strategy*, 338.

[46] Ibid., 334.

[47] Cited in Jerome V. Martin, *Victory From Above: Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm* (Maxwell AFB, AL: Air University Press, June 1994), 24.

[48] Mark Garrard, "War Termination in the Persian Gulf: Problems and Prospects," *Aerospace Power Journal* 15, no. 3 (Fall 2001), 5.

[49] Stanley T. Kresge, *Gulf War Termination Revisited* (Maxwell AFB, AL: Air University, April 1999), 22–23.

[50] G.H. Bowdey, *The Nature of Naval Warfare* (Newport, RI: Naval War College, 1938), 12.

[51] Otto Groos, *Seekriegslehren im Lichte des Weltkrieges. Ein Buch für den Seemann, Soldaten, und Staatsmann* (Berlin: E.S. Mittler & Sohn, 1929), 23; Hein-Peter Weyher, *Der Begriff "Seestrategie" und Seine Deutung in den Westlichen Kriegstheorien Des 20 Jahrhunderts* (Hamburg: Führungsakademie der Bundeswehr, July 1967), 11.

[52] Nish, "The Russo-Japanese War," 12.

[53] Ibid.

[54] Hamby, "Striking the Balance," 335.

[55] Philip Wasielewski, *The Evolving Political-Military Aims in the War in Ukraine After 100 Days* (Philadelphia: Foreign Policy Research Institute, June 2022), 2.

[56] Riley Bailey et al., *Russian Offensive Campaign Assessment, December 30* (Washington, DC: Institute for the Study of War, December 2022), 3–6, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-december-30.

[57] Wasielewski, *The Evolving Political-Military Aims in the War in Ukraine After 100 Days*, 5.

[58] Martin Armstrong, "Liberated Ukrainian Territory," *Statista*, November 18, 2022, 1, https://www.statista.com/chart/28748/ukraine-territory-control-status-distribution/.

[59] Wasielewski, *The Evolving Political-Military Aims in the War in Ukraine After 100 Days*, 5.

[60] Malcolm W. Cagle and Frank A. Manson, *The Sea War in Korea* (Annapolis, MD: Naval Institute Press, 1957), 116.

[61] Norbert Hanisch, *Untersuchen Sie die operativen Ideen Manstein hinsichtlich Schwerpunkt-bildung, Überraschung, Initiative und Handlungsfreiheit an den Beispielen Westfeldzug 1940 (Sichelschnitt-Plan) und Operation Zitadelle* (Hamburg: Führungsakademie der Bundeswehr, January 15, 1988), 33; *Die Operative Kunst der Luftstreitkräfte*, Part 1 (Dresden: Military Academy Friedrich Engels, 1976), 119.

[62] *Sound Military Decision Including the Estimate of the Situation and the Formulation of Directives* (Newport, RI: Naval War College, 2012), 158.

[63] The Prussian general and reformer Gerhard von Scharnhorst (1755–1813) was reportedly the first to use this term in his discussion on the operations. Scharnhorst repeatedly referred to the factors of space (*Raum*), time (*Zeit*), forces (*Kräfte*), and means (*Mitteln*). Hansjürgen Usczeck, *Scharnhorst. Theoretiker, Reformer, Patriot* (East Berlin: Militärverlag der Deutschen Demokratishen Republik, 1979), 138–140. This concept became part of the Prussian/German military thinking after General Helmuth von Moltke, Sr., became chief of the Prussian General Staff in October 1857. In 1865, he directed that the calculation of space, time, and means be the foundation of all General Staff work. See Volker Wieker, *Operation, Operative Führung zwischen Taktik und Strategie—Bedeutung und Entwicklung des Begriffes seit Moltke d. Ae.—Bearbeitung aus der Sicht der Landstreitkräfteführung* (Hamburg: Führungsakademie der Bundeswehr, December 12, 1988), 8.

[64] *Operative Leitlinie für die Führung von Landstreitkräften* (Hamburg: Führungsakademie der Bundeswehr, August 1992), 2.

[65] Peter Wenning, *Aufmarschplanung als strategische Führungsproblem. Eine vergleichende Untersuchung am Beispiel des Schlieffenplans 1914, der NATO Aufmarschplanung im Rahmen der "Flexible Response" un dem neuen strategischen Konzept der NATO* (Hamburg: Führungsakademie der Bundeswehr, December 30, 1997), 11.

[66] Tim Bouverie, *Appeasers: Chamberlain, Hitler, Churchill, and the Road to War* (New York: Tim Duggan Books, 2019), 365, 377.

[67] Kotoulas and Pusztai, *Geopolitics of the War in Ukraine*, 32.

[68] Forrest C. Pogue, *United States Army in World War II. The European Theater of Operations: The Supreme Command* (Washington, DC: U.S. Army Center of Military History, 1989), 53; *Report by the Supreme Commander to the Combined Chiefs of Staff on the Operations in Europe of the Allied Expeditionary Force 6 June 1944 to 8 May 1945* (Washington, DC: U.S. Army Center of Military History, 1994), v.

[69] William D. Ivey, *Objectives and Success: Linking National Policy Objectives and Military Strategic Objectives to Achieve Success* (Carlisle Barracks, PA: U.S. Army War College, 1996), 7.

[70] Ibid., 8.

[71] Jim Garamone, "Rumsfeld Lists Operation Iraqi Freedom Aims, Objectives," *AF.mil*, March 21, 2003, https://www.af.mil/News/Article-Display/Article/139787/rumsfeld-lists-operation-iraqi-freedom-aims-objectives/.

Custer's Last Stand, by Edgar Samuel Paxson, oil on canvas, 1899 (Courtesy Whitney Gallery of Western Art)

Applying Three Decisionmaking Models to the Lakota Sioux Wars

By Jacob Ivie and Bradley F. Podliska

A core responsibility of a leader, whether it be the President of the United States, a general officer in the military, or a newly commissioned second lieutenant, is decisionmaking. Leaders, set with their own perceptions of the world, biases, motivations, and values, are trying to resolve the uncertainty of the future by planning. In this situation, leaders do not have the advantage of hindsight, which provides clarity when analyzing a decision. Hindsight or any post hoc analysis allows for an understanding of the facts and circumstances surrounding a decision—all without temporal pressure or the fog of war to impede adequate processing.[1] For example, most students of war would agree that General Robert Lee's decision to order Pickett's charge and Adolf Hitler's decision to attack the Soviet Union were imprudent and arguably led to the demise of their respective armies.

Leaders, however, do have an ex ante tool at their disposal—decision strategies—and these strategies offer a structure to make an objective analysis—one that can explain a decision, a prediction, or even both. More

Major Jacob Ivie, USAF, is Director of Wing Inspections at the 552nd Air Control Wing. Bradley F. Podliska is an Assistant Professor of Military and Security Studies at the Air Command and Staff College.

Sitting Bull, cabinet card, Bismarck, Dakota Territory, circa 1883 (David F. Barry)

specifically, leaders can use one of three prominent decision strategies—expected utility, cybernetic, or poliheuristic—as a tool to understand, analyze, and resolve complicated situations.

These strategies are best exemplified as a case study. While they can be applied to any battle, the war between the U.S. Army and the Lakota Sioux during the Black Hills Campaign, given the series of decisions by three very different individuals, offers an exemplary historical event for examination. In particular, the strategies can be applied to the June 1876 decisions of Crazy Horse, Lieutenant Colonel George Custer, and Major Marcus Reno.[2]

The following paragraphs take the reader through three case studies applying varying decision strategies using cognitive and subjective, as well as rational and objective, patterns of behavior. The analysis provides a construct to explain the reasons why Crazy Horse attacked Brigadier General George Crook at the Battle of Rosebud, why Custer ignored multiple advisors and attacked the numerically superior Lakota Sioux people at the Little Bighorn River, and why Reno decided to halt his offensive movement and establish defensive pickets at the beginning of Little Bighorn. More important, the analysis provides scenarios in which the reader can compare patterns of behavior unique to each leader. The connections between personalities and histories of behavior reveal patterns that may be used as tools for current leaders to link past actions, assess current actions, and predict future actions.

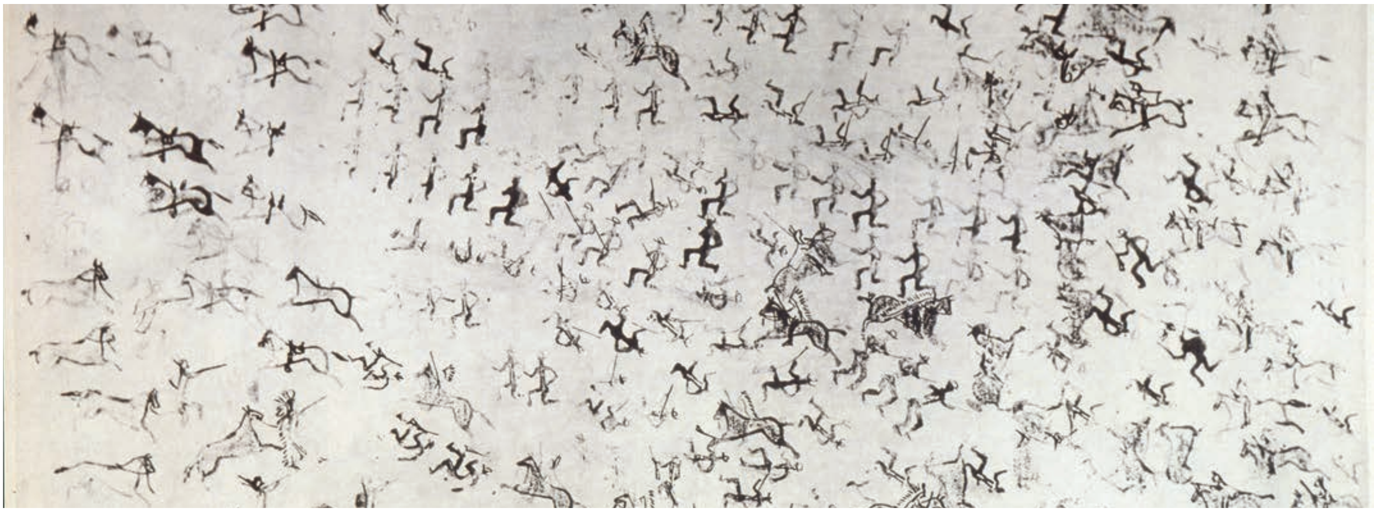
Decision Strategies

To assist in understanding and making optimal decisions, decisionmakers have tools and structure in the form of three decision strategies: expected utility, cybernetic, and poliheuristic.

First, *expected utility* is a holistic approach to decisionmaking that weighs all factors to maximize the total value and identify the most desirable outcome.[3] These factors are compensatory, which means that a high value in one can compensate for a low value in another. A primary assumption under this theory is that decisionmakers are rational, but because all humans are unique, not all leaders will assign the same utility to the same factors.[4] Since leaders have varying thresholds for how much risk to assume, decisions may vary but will remain rational relative to the decisionmaker's preferences.[5] The expected utility decision strategy weighs the values of options against the probability of outcomes to mathematically calculate the decision that provides the most benefit.

Cybernetic, the second decision strategy, is a nonrational, cognitive approach that relies on intuition and experience. While the cognitive process associated with a cybernetic approach is complex, the goal is to make the decision process as simple as possible by eliminating uncertainty and resolving ambiguity.[6] The leader makes a "good enough" decision often due to temporal constraints. Although a strength of this approach is timeliness, cybernetic processing is less predictable than expected utility and does not assess all factors. In fact, cybernetic decisions are often made based on past data, a psychological principle known as *reinforcement*.[7] Thus, a leader's experience and personality heavily influence outcomes when applying the cybernetic approach.

The third decision strategy is a *poliheuristic* approach that combines rational and cognitive processing in a two-stage model. The first stage is noncompensatory and cognitive, since the decisionmaker has multiple factors to consider, but eliminates those options with characteristics that are dealbreakers. These factors, or "dimensions," as Alex Mintz describes them, are



Native American depiction of Battle of Little Bighorn, June 25, 1876 (Amos Bad Heart Bull, also known as Wanbli Waphaha [Eagle Bonnet], ca. 1868–1913—noted Oglala Lakota artist in Ledger Art)

noncompensatory in that no degree of positivity in other factors will compensate for the negative quality of the noncompensatory dimension.[8] Notably, the decisionmaker may encounter multiple levels of noncompensatory dimensions in the decision process. After decisionmakers eliminate options containing qualities in the noncompensatory dimension, they are left with either one option or multiple options in the compensatory dimensions during the second stage. These dimensions may then be assigned values of expected utility and rationally assessed to assign an overall value for each option.[9] For example, leaders often subjectively eliminate any option that could result in termination from their position and then objectively assess the remaining options.

The Black Hills Battles of the Lakota Sioux Wars

The war between the Lakota Sioux and the U.S. Army during the summer of 1876 provides a case study for examining each of these decision strategies. The situation leading up to the battles had been mostly peaceful since the Fort Laramie Treaty of 1868 was signed, establishing the Dakota territories west of the Missouri River as the Great Sioux Reservation. The treaty allowed the Sioux to hunt outside the borders but forbade "occupation" of the lands beyond.[10] Conflict arose in 1873 after a financial panic, when miners, seeking gold, sneaked into a remote area of the reservation called the Black Hills. The Army appointed Custer to lead an expedition in 1874 to determine the quantity of gold in the region. His report was highly favorable, so President Ulysses S. Grant, determined to pay off the national debt, attempted to buy back the land from the Sioux, but the tribe refused to agree to the price. As miners began to flood into the area, Grant relied on exaggerated reports of violations by the Sioux to issue an ultimatum to all the "wild" bands to leave their hunting grounds by January 31, 1876. The Sioux, understandably, did not comply, and minor skirmishes turned into a full-fledged war between the Army and the Lakota Sioux.[11]

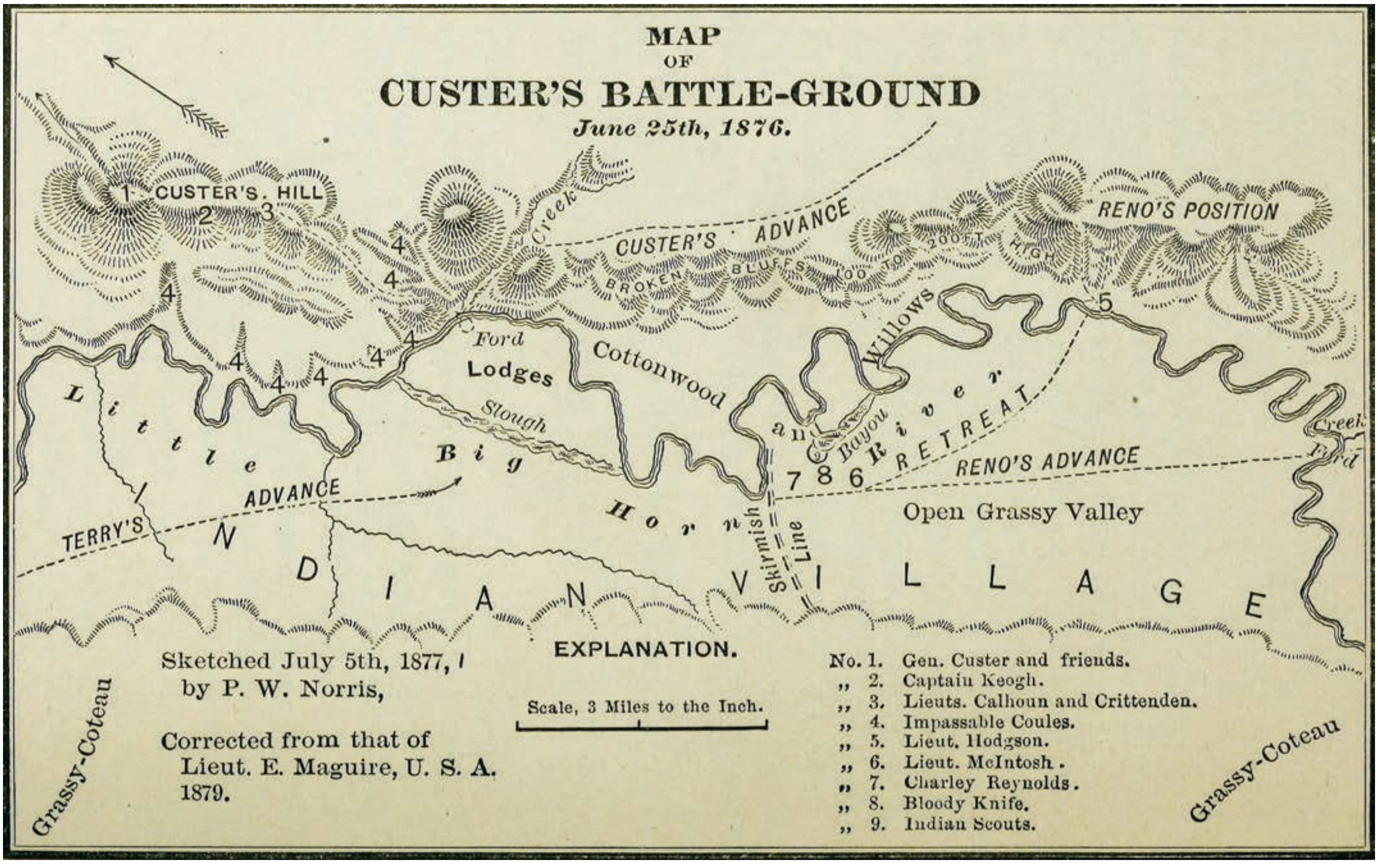
Crazy Horse and George Crook. The first case study involves Crazy Horse's decision to attack General Crook's forces at the Battle of Rosebud, on June 17, 1876. By this time, the United States had launched a three-prong offensive to find and eradicate any Sioux in the Black Hills. General John Gibbon came from Fort Ellis, Montana, in the west, while General Alfred Terry came from Fort Lincoln in the east, accompanied by Custer and the Seventh Cavalry. Crook's column of about 1,000 men came from the south. All the commanders knew the Sioux were trapped in the area but had difficulty precisely locating the warriors.[12] On the evening of June 16, following a Sun Dance ritual, Sitting Bull and Crazy Horse were camped on Ash Creek and received a report from Cheyenne scouts that "Three Stars" (Crook) was coming north.[13] Since Sitting Bull was greatly fatigued from cutting himself for a blood sacrifice, staring at the sun, and dancing to the point of unconsciousness, Crazy Horse was the leader suitably fit to make a decision to attack or evade.[14]

A brief description of Crazy Horse's personality enhances understanding of his thought process. His parents were an Oglala Lakota also named Crazy Horse and a Miniconjou Lakota named Rattling Blanket Woman. The son was raised to be patient out of necessity since his father was a medicine man and did not have the traditional duties within the tribe, especially as a hunter. His childhood was riddled with persecution for his having light hair and being the son of a medicine man. This turmoil gave him a unique perspective.[15] For example, Crazy Horse was more prudent during the Sun Dance and did not overexert himself, a testament to his character as one of pragmatism and humility. While other Sioux displayed full headdresses of eagle feathers, each a symbol of killing or touching an enemy in combat, he rarely displayed more than one or two, even though his father reported he had killed over 30 men.[16] Crazy Horse was also a planner, but his desire for well-laid plans was often overruled in circumstances created by younger, more zealous warriors. One such example was in the Yellowstone Valley in August 1872, when his band of warriors discovered Major Eugene M. Baker's Second Cavalry. Crazy Horse wanted to plan a careful attack, but the young warriors could not resist the temptation of capturing the rations and horses, resulting in a hastily conducted attack. Losing the element of surprise, Crazy Horse angrily ordered a withdrawal and left the area empty-handed.[17] He faced a similar situation 4 years later at Rosebud.

Early on the morning of June 16, Crook departed Goose Creek with a sizable force of 975 Soldier combatants and 250 auxiliaries from the U.S.-aligned Crow and Shoshone tribes.[18] His objective was to find and destroy a strong Lakota village in the area. Shortly after departing, the column crossed paths with a fleeing buffalo herd, which led to the discovery of an abandoned camp containing a wickiup (hut) with partially cooked buffalo meat.[19] After a hard day's ride, and suspicious that Crazy Horse had seen the column, Crook ordered a cold bed-down with no fires and orders to move out at 4:30 a.m. the next day. The column moved out on time and followed the South Fork of Rosebud Creek to the northeast. At 8 a.m., the scouts reported seeing mounted Sioux. The report was ambiguous but enough to make Crook halt the column and dismount the cavalry to set up picket lines.[20] The Soldiers took this opportunity to relax and casually sprawl out for about an hour and a half before hearing gunfire. Initially, most Soldiers thought the Crow and Shoshone scouts were firing at buffalo, until the scouts appeared riding as fast as they could with hostiles pursuing them.[21]

Shortly after noon on June 16, the Cheyenne scout Little Hawk, who was loyal to the Lakota Sioux, pursued what he thought were other friendly Sioux only to discover Crook's entire column on a march near the head of the Rosebud. He immediately set out to report the location of Crook's column to Crazy Horse and Sitting Bull, who were encamped at an enormous village at what is known today as Reno Creek.[22] The two Sioux leaders were initially inclined to avoid contact, but the clamor from the younger warriors made them realize that a clash was inevitable.[23] This decision point reflects the first noncompensatory stage of Crazy Horse's use of a poliheuristic approach. The noncompensatory dimension was the morale of his warriors and his honor and prestige as a warrior-leader. He eliminated any option to evade and not attack because he needed to appease his warriors, who were in high spirits and anxious to fight, and to preserve his honor as a leader of the Lakota.

Crazy Horse then entered the second stage of the poliheuristic model. Once he decided to move out, there were two considerations that emerged. The first was how many warriors he would take to confront Crook. Some advised to move every warrior toward Crook's forces,



"Map of Custer's Battle-Ground," in Philetus W. Norris, *The Calumet of the Coteau, and Other Poetical Legends of the Border* (Philadelphia: J.B. Lippincott and Co., 1883), 42 (U.S. Army/P.W. Norris and E. Maguire/Library of Congress) but Crazy Horse knew if he took all the warriors, he would leave the women and children unprotected.[24] The second consideration was whether to set up a defensive line to intercept Crook's column or to offensively attack Crook wherever he and his warriors would happen to find Crook's column. Understanding that he had to act and act quickly, Crazy Horse was faced with four options: take all the warriors and set up a defensive line, take all the warriors and assume the offensive, leave a portion in reserve and set up a defensive line, or leave a portion in reserve and assume the offensive.

Using the poliheuristic model, these four options require dimensions against which to measure utility and weigh the options. The first dimension is protecting the women and children. Taking all the warriors has a low utility since the innocents would be unprotected, while leaving reserves receives a higher score in this first dimension regardless of the offensive or defensive option. The second dimension involves gaining and retaining the initiative. Setting up a defensive line inherently gives up the initiative, while sending all the troops might require more time and a smaller contingent would be more expeditious. The third dimension is the level of stealth required to achieve the element of surprise. The ability to remain concealed decreases as the number of warriors increases, making the option to take all the warriors have a lower utility in this third dimension. Inversely, defensive operations inherently favor concealment and stealth, giving the defensive option higher utility than the offensive one. The fourth dimension is reputation—not just for Crazy Horse, but for all the warriors. Native American culture is rife with honor and tradition, which would tip the scales of utility toward an offensive attack, while the honor of protecting the elders also carries heavy weight. The fifth and final dimension is force ratio. Higher numbers increase the probability of overall mission success, making the option to take all the warriors more desirable, while force ratio also benefits the defense over the offense. Table 1 below depicts five dimensions Crazy Horse likely considered in his decision and numerical values based on estimated utility for each option (1 to 5, with 1 representing low utility and 5 representing high utility). The calculation reveals that leaving a reserve force and using the remaining warriors to mount an offensive has the highest utility of 18.

The Battle of Rosebud started on the morning of June 17, with Crazy Horse

Major General George Armstrong Custer, May 1865 (Library of Congress/National Archives and Records Administration/Mathew Brady)

Table 1.

	Defense w/ All Warriors	Offense w/ All Warriors	Defense & Leave Reserves	Offense & Leave Reserves
Protection of Weak	1	1	5	5
Initiative	2	5	2	4
Stealth	2	1	4	3
Reputation	1	3	2	4
Force Ratio	5	4	3	2
Sum	11	14	16	18

The Custer Fight, by Charles Marion Russell, lithograph showing Battle of Little Bighorn from the Native American side, 1903 (Library of Congress, with restoration by Adam Cuerden)

having the element of surprise after a night march to Rosebud and a short rest between dawn and about 8:30 a.m., when he resumed his march.[25] He opted to leave a portion of his forces behind and aggressively seek out Crook's column with the remaining forces numbering approximately 750.[26] The battle raged for 6 hours with warriors attacking and withdrawing, giving the women and children back at camp time to escape. Although Crook reported this battle as a victory since he successfully drove Crazy Horse's warriors from the field, it was a strategic loss. Crook did not find the Sioux encampment and abandoned his mission. Worse yet, he did little to pursue the warriors and failed to report accurate numbers, strength, and tactics to Terry and Gibbon, depriving Custer of critical intelligence.[27]

Custer's Blunder. The second case study exemplifies the cybernetic processes underlying Custer's decision to attack the Sioux camp at the Battle of Little Bighorn. This case study begins with an examination of Custer's personality to lay a foundation for understanding his cognitive decisionmaking. Custer was an extroverted individual who had vast experience fighting the native peoples, thought of the frontier as one huge adventure, and was viewed as aloof and insubordinate by many superiors. During the Civil War, Custer was a fearless and sometimes reckless combatant underpinned by his sense of divine protection from death, as indicated in a letter to his wife, Libbie, in May 1864. In the letter, he attributed his self-proclaimed bravery to his destiny being in the "hands of the almighty."[28] Custer's first experience after the close of the Civil War was on the Great Plains in 1867 under General Winfield Hancock. Hancock's heavy hand when dealing with the native tribes set up circumstances where Custer was unsuccessful and lost favor with his superiors. This failure, coupled with problems of desertion and separation from Libbie, were reasons that Custer used to justify leaving his command and traveling 150 miles to see her. As a result, he faced a court-martial and lost his command for a year.[29]

Custer was desperate to repair his reputation and, with the help of General Terry, eventually achieved reinstatement and headed to Fort Hayes, Kansas.[30] His first engagement after being reinstated was in Oklahoma at the Washita River in November 1868, where young warriors from the friendly tribes were conducting raids into Kansas. Custer, commanding about 800 men, successfully tracked down a band of raiders, divided his forces into four even detachments, and surrounded their camp. In less than an hour and without the aid of reconnaissance, Custer's Soldiers killed over 100 warriors; 1 U.S. Soldier was killed, and 13 were wounded.[31] Custer had proved to his superiors that he was competent. In the years to follow, he wrote his wife long letters about his adventures on the Plains, recalling one extended march in 1873 as being "perfectly delightful thus far," while his superior, Colonel David S. Stanley, who complained about being wet for 9 days straight, referred to Custer as "untruthful and unprincipled."[32]

On June 23, 1876, about a week after Rosebud, Custer's Seventh Cavalry rode west ahead of Terry in search of the hostiles. Along the 33-mile trek, they found the remains of campsites indicating they were on the trail of a large group of Lakota Sioux. Around 4:30 p.m., they stopped to camp along the east side of the Rosebud

River to allow the pack mules to catch up.[33] The next day, the column found even more abandoned encampments, but these were fresher than those discovered the previous day. By 1 p.m., Custer called another halt to assess the situation. He received a report that there might have been a trail 10 miles back that had been overlooked, so he sent scouts back but also sent some scouts forward to reconnoiter the path ahead. About 3 hours later, the scouts returned with two pieces of news.

First, the overlooked trail 10 miles back was a detour that joined with the main trail they had been traveling. Second, along the main trail 12 miles ahead was a fresh camp, indicating that a massive Sioux encampment was no more than 30 miles ahead.[34] At 5 p.m., they resumed their march, finding more camps with smoldering fires, and at 7:45 p.m. they halted on the west side of the Rosebud. By 9 p.m., scouts reported that the trail broke from the Rosebud and led to the valley of the Little Bighorn. The Sioux encampment was closer than Terry had predicted, and Custer had a decision to make.[35]

Terry ordered Custer to march southward and then westward if the trail turned away from the Rosebud, but he left a loophole by adding, "unless you see sufficient reasons [for] departing from [the orders]."[36] What constituted "sufficient reasons" in this case is debatable, but the hostiles were so close that marching southward was likely to expose, or might have already exposed, the column of 600 men. Additionally, the long march would delay Custer until June 27, and Terry could arrive as early as June 26. Custer saw this as a golden opportunity to avoid the ridicule and courts-martial other officers had endured after allowing the Sioux to escape.[37] Thus, Custer decided to "disobey" orders and follow the trail on the morning of June 25, when his scouts informed him that they had spotted the hostile village. The scouts stated they could also see the campfires of the column from their lookout point. Many of Custer's men agreed that his position had been compromised, even though the only proof was a pair of Sioux riders who had been seen briefly before disappearing.[38] Notably, no less than five trusted men warned Custer that a great number of hostiles were at the encampment. One Crow scout even told Custer that there were too many to fight with all the men at his disposal, urging him not to divide his forces.[39] Yet Custer acted completely opposite, dividing 12 companies into 3 divisions to attack along multiple axes without Terry's reinforcements.

Custer's decision to attack was cybernetic for four reasons. First, he sought to eliminate the uncertainty of whether the Seventh Cavalry under his command would reap the glory of eradicating the Sioux threat before it dispersed. Delay might cause the encampment to disperse, robbing Custer of the opportunity to improve his reputation. Second, he fell victim to a cognitive bias known as *social corroboration*, where decisionmakers "bolster their judgments by the concurring opinions of other people."[40] His scouts convinced Custer that his position had been compromised despite the lack of evidence.

Third, inferences of transformation or wishful thinking played a role by allowing Custer to cognitively dismiss the repeated warnings of multiple eyewitnesses who swore there were more warriors than the unit could handle. This notion of superior numbers was inconsistent with previous encounters and, even if true, would, as Custer thought, play out favorably over time.[41] When Bloody Knife stated there were enough Sioux to "keep us fighting two or three days," Custer's response was, "I guess we'll get through them in one day."[42] This aloof response shows that rational decision processes had given way to predilections in Custer's mind. The fourth reason is an example of the cognitive concept of reinforcement.[43] Custer's success at Washita was based on two factors: the element of surprise and dividing his forces. Thus, he based his decision to divide forces on the idea that past success would surely lead to future success. He assigned companies D, H, and K to Captain Frederick Benteen, who immediately rode to the left to sweep the area for Sioux while Custer took companies C, E, F, I, and L and continued toward the Little Bighorn valley with Reno's A, G, and M companies.

Reno's Encounter. The last case study is Reno's expected utility decision to set up a defensive skirmish line at first contact with the southern flank of the Sioux camp. Reno had served with minimal distinction during the Civil War and joined the Seventh Cavalry after Washita in 1868. He was known as a humorless person who favored the bottle and was not well liked by his fellow officers, but he was cautious and prudent in his decisionmaking.[44] Reno and Custer followed a small tributary named Ash Creek (now Reno Creek) to a point where they split; Reno crossed the Little Bighorn River and advanced to the left following an order to pursue a band of 50 fleeing Sioux, while Custer continued along a bluff on the right side of the river opposite the encampment to attack from the north.[45] When Reno approached the village, he saw that there were significantly more warriors than he or Custer had anticipated. Custer had not relayed his intentions to attack the north but rather had told Reno he had Custer's support. Reno was left with a decision to continue the charge into a possibly overwhelmingly larger force or to set up a defensive skirmish line. He opted for the latter.[46]

Reno's situation exemplifies the expected utility method of decisionmaking based on the probability of whether the opposing force was overwhelming. The common force ratio of three to one is traditionally required for an attacking force and will be used to define *overwhelming* in this case (see table 2). If Reno assigned a 70 percent chance that

Table 2.

	A) Overwhelming 70% (.7)	B) Manageable 30% (.3)	Sum
Charge	2(.7) = 1.4	8(.3) = 2.4	1.4 + 2.4 = 3.8
Defend	6(.7) = 4.2	4(.3) = 1.2	4.2 + 1.2 = 5.4

the forces ahead would be overwhelming, as depicted in columns A and B, he would have then weighed the probability against the options to charge or defend (rows 1 and 2) by computing expected utility values from 1 to 10 for each of the four outcomes. Charging in the face of an overwhelming force (1A) has the lowest value of 2 because of the inability to counterattack and likelihood of being surrounded. Charging against a manageable force (1B) has a high value of 8 because it accomplishes the mission without annihilation. Setting up a defensive skirmish line against an overwhelming force (2A) has a value of 6 because the Sioux could have time to scatter, but it increases the likelihood of survival and reinforcements. Defending against a manageable force (2B) has a value of 4, since the opportunity to seize the initiative is lost but the options for a counterattack and pursuit remain. Tallied totals show the defense option with a value of 5.4 is greater than the value of 3.8 for the option of charging. The decision to set up a defensive line reflects the holistic and rational approach of the expected utility process.

Conclusion

The outcome of the Battle of Little Bighorn varied greatly for the three leaders. Reno's move from the south came as a surprise to Crazy Horse, who was expecting Custer but had not seen Reno break off. But because Reno's men were so tired, they were unable to hold and were forced to retreat back across the Little Bighorn.[47] About half of Reno's unit finally managed to occupy the bluff where Reno had last seen Custer and take up a defensive position.[48] Eventually, Benteen arrived and rescued Reno and what remained of his three companies, but neither Reno nor Benteen knew Custer's location.[49] Custer, having seen Reno's advance, took his five companies over the hill, never to be seen again.[50] Debates resound about the details, but evidence points to at least two companies making it to the river before the entire force was repelled and devastated at the high ground north of the Little Bighorn, where monuments exist now. When Reno attacked, Crazy Horse was at the encampment and led a group of warriors across the river to assist in the destruction of Custer's five companies.[51] The speculation varies as much as the personalities involved, but Sitting Bull revealed in an interview years after the battle that "the Long Hair [Custer] stood like a sheaf of corn with all the ears fallen around him."[52]

Examining the factors leading to the decisions made by Crazy Horse, Custer, and Reno through the lenses of expected utility, cybernetic, and poliheuristic decision strategies enables objectivity in analysis and hindsight. It also offers an example of how to study three different leaders, each of whom resolved uncertainty with their decisions, even if such decisions proved disastrous. Modern leaders can utilize these same tools to make sense of complexity and to apply a framework to analyze an opponent's past decisions, compare the findings to the present situation, and then predict future courses of action. JFQ

Notes

[1] David Hackett Fischer, *Historians' Fallacies: Toward a Logic of Historical Thought* (New York: Harper & Row, 1970).

[2] Although Custer held the rank of brevet major general during the Civil War, his rank of lieutenant colonel is used for reference to command relationships with superiors and subordinates.

[3] Bruce Bueno de Mesquita, *The War Trap* (New Haven: Yale University Press, 1981), 20, 30.

[4] Ibid., 29.

[5] Ibid., 31.

[6] John D. Steinbruner, *The Cybernetic Theory of Decision: New Dimensions of Political Analysis* (Princeton: Princeton University Press, 1974), 51, 88–89.

[7] Ibid., 112–114.

[8] Alex Mintz, "How Do Leaders Make Decisions? A Poliheuristic Perspective," *Journal of Conflict Resolution* 48, no. 1 (February 2004), 6–8; Alex Mintz, "The Decision to Attack Iraq: A Noncompensatory Theory of Decision Making," *Journal of Conflict Resolution* 37, no. 4 (December 1993), 599–600.

[9] Ibid., 597.

[10] James Donovan, *A Terrible Glory: Custer and Little Bighorn, the Last Great Battle of the American West* (New York: Little, Brown and Company, 2008), 28–29.

[11] Ibid., 32–36.

[12] Stephen E. Ambrose, *Crazy Horse and Custer: The Parallel Lives of Two American Warriors* (New York: Anchor Books, 1996), 417–419.

[13] Ibid., 417.

[14] Thomas Powers, *The Killing of Crazy Horse* (New York: Vintage Books, 2010), 174.

[15] Joseph M. Marshall III, *The Journey of Crazy Horse: A Lakota History* (New York: Penguin Books, 2005), 4, 14.

[16] Ibid., 31.

[17] Ambrose, *Crazy Horse and Custer*, 353.

[18] Paul L. Hedren, *Rosebud, June 17, 1876: Prelude to the Little Bighorn* (Norman: University of Oklahoma Press, 2019), 155.

[19] Ibid., 159.

[20] Ibid., 161–163.

[21] Ibid., 165.

[22] Ibid., 168–170.

[23] Powers, *The Killing of Crazy Horse*, 175.

[24] Ambrose, *Crazy Horse and Custer*, 417.

[25] Ibid., 420–421.

[26] Hedren, *Rosebud, June 17, 1876*, 176.

[27] Donovan, *A Terrible Glory*, 153–154.

[28] Kevin M. Sullivan, *Custer's Road to Disaster: The Path to Little Bighorn* (Guilford, CT: TwoDot, 2013), 38.

[29] Ibid., 57–58.

[30] Ambrose, *Crazy Horse and Custer*, 404.

[31] Ibid., 311–321.

[32] Ibid., 357–359.

[33] Donovan, *A Terrible Glory*, 195–196.

[34] Ibid., 196–197.

[35] Ibid., 197–198.

[36] Ambrose, *Crazy Horse and Custer*, 427.

[37] Donovan, *A Terrible Glory*, 199.

[38] Ibid., 207.

[39] Ibid., 212.

[40] Steinbruner, *The Cybernetic Theory of Decision*, 121.

[41] Ibid., 116–117.

[42] Donovan, *A Terrible Glory*, 206.

[43] Steinbruner, *The Cybernetic Theory of Decision*, 113–114.

[44] Donovan, *A Terrible Glory*, 93.

[45] Michael N. Donahue, *Drawing Battle Lines: The Map Testimony of Custer's Last Fight* (El Segundo, CA: Upton and Sons Publishers, 2008). See hand-drawn map by Frederick Benteen, 66.

[46] Donavan, *A Terrible Glory*, 228–229.

[47] Ambrose, *Crazy Horse and Custer*, 438–439.

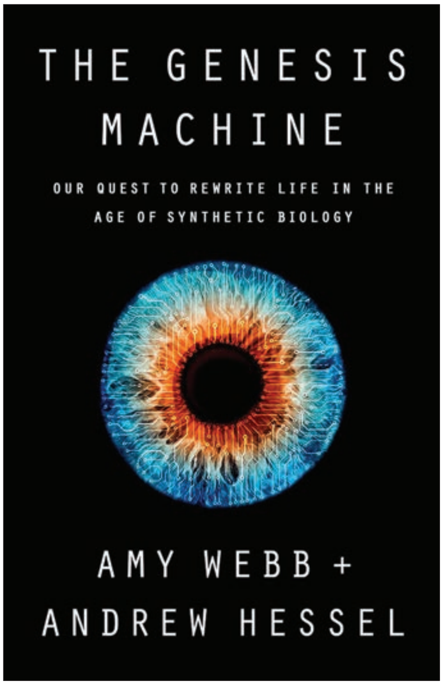
[48] Donovan, *A Terrible Glory*, 238.

[49] Ibid., 259.

[50] Sullivan, *Custer's Road*, 165.

[51] Ibid., 170.

[52] Stephen Brennan, ed., *An Autobiography of General Custer* (New York: Skyhorse Publishing, 2012), 279.



The Genesis Machine: Our Quest to Rewrite Life in the Age of Synthetic Biology

By Amy Webb and Andrew Hessel
New York: PublicAffairs, 2022
368 pp. $29
ISBN: 978-1541797918

Reviewed by Diane DiEuliis

Emerging biotechnologies, particularly as the COVID-19 pandemic recedes, have captured the imagination, interest, and concerns of the world. Scenarios once relegated to science fiction movies and novels are now potentially within the grasp of bioengineering: the ability to read, write, and edit DNA—the fundamental code of life. The purposeful design of biology can enable novel ways to meet a variety of societal needs—from the biomanufacturing of commodities to gene therapies and the recreation of once-extinct organisms. This biological revolution, or "bioeconomy," has the potential to address important issues such as climate change, sustainable energy, and food production, as well as improved medicines and quality of life for all. But with this capability comes dual use (that is, not only for commercial/military use but also by good actors/bad actors) as well as profound ethical concerns, making *The Genesis Machine* a timely volume.

The authors—Amy Webb, a journalist and futurist, and Andrew Hessel, a pioneering geneticist—begin their story in personal terms, each revealing how the adoption of biotechnologies in her or his own life has been transformational in enabling her or him to have families. This sets the stage for a well-narrated journey through the history of biotechnology progress, from early pharmaceutical triumphs such as insulin to the synthetic biological creation of artemisinin, which is used in the treatment of malaria. For those new to biotechnology as well as those who work in the field, the personal stories of those involved in the earliest discoveries that punctuated disruptive progress in the life sciences are one of the most entertaining aspects of the book. The anecdotes surrounding serendipitous discoveries, along with the quirks of biotechnology's most famous pioneers, are not commonly known and give great depth to this historical background.

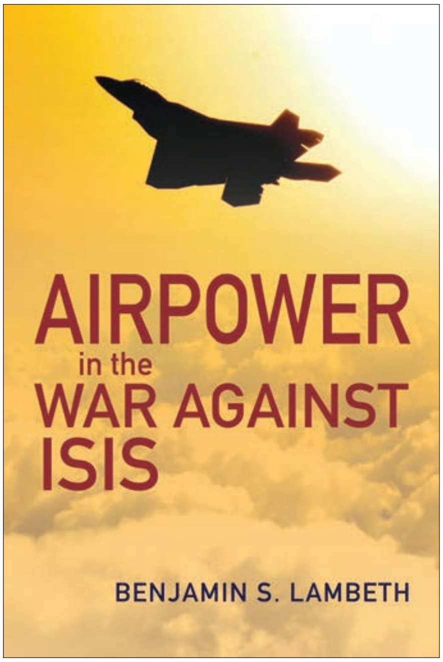
With this foundation, Webb and Hessel launch into the varied potential of bioengineering and provide helpful background on the components of the bioeconomy, including some discussion of the dual-use concerns associated with these possibilities. Although the book does touch on some of the "non-life sciences" outputs of the bioeconomy, such as biofuels or DNA as digital data storage, it is primarily focused on the human impacts of bioengineering. The authors focus throughout on medicine, health, reproduction, and agriculture—the primarily "traditional" sectors in which biotechnology exists. However, biotechnologies are more likely to commercially advance (in the near term) with biomanufacturing—moving from petroleum-based platforms for manufacturing to biologically based ones—and how this affects the planet will be important. Another missing scenario might be the unknown ecological consequences of the reintroduction of an extinct species, like the woolly mammoth, for example, for which efforts are already under way. This does not detract from the book, however, given that there is much to be learned from the human-impact scenarios described—the scenarios are as fascinating to entertain as they are ethically challenging and would make for creative discussions in the classroom.

The Genesis Machine provides some windows into the current policy landscape and highlights most current governance; however, this book should not be construed as a treatise on policy or a primer for would-be life sciences policymakers. It does not describe how biodefense or biosecurity policy evolved in reaction to biotechnology advances, which is the parallel understanding needed to understand why current policy may be inadequate and where gaps exist. Similarly, although it discusses dual use, it does not dive into weapons scenarios, nor does it touch on the different broad spheres of thought on how best to navigate life sciences policy and governance: ideas such as self-governance, risk-benefit assessment, or the precautionary principle. The best use of this book is as a highly accessible primer on biotechnology and as a tool to stimulate general awareness-raising of its ethical use in the human dimension.

Given that biotechnology is a "modernization priority" for the Department of Defense (DOD), this book may offer insights for readers and students in the joint force. Soon, emerging biotechnology will affect Servicemembers and how DOD performs its mission, from bioproduced and bioinspired materials to novel sensors and pharmaceuticals. Importantly, some of the most powerful and potentially controversial uses of emerging biotechnology and synthetic biology will be on human performance—in the U.S. military as well as in those of its adversaries. An awareness and understanding of these kinds of impacts will be needed across the joint force community, and this book offers an entrée into the field.

Overall, *The Genesis Machine* is an enjoyable and well-researched read. It provides a smooth narrative overview of many of the challenges of the biotechnological age that would provide novice students, general readers, and experts alike with a balanced foundation in understanding the impacts of biotechnology on humanity—and a thought-provoking tool for imagining life on the planet in the coming decades. For those in the joint force with roles in emerging technology and modernization priorities, this book deserves a space on the bookshelf. JFQ

Dr. Diane DiEuliis is Assistant Director and Distinguished Research Fellow in the Center for the Study of Weapons of Mass Destruction, Institute for National Strategic Studies, at the National Defense University.



Airpower in the War Against ISIS

By Benjamin S. Lambeth
Annapolis: Naval Institute Press, 2021
352 pp. $55
ISBN: 978-1682475577

Reviewed by Charles J. Dunlap, Jr.

In *Airpower in the War Against ISIS*, Benjamin Lambeth not only weaves an account that celebrates the decisive role he insists airpower played in the defeat of the so-called Islamic State (IS) but also depicts tragically missed opportunities and almost incomprehensibly poor judgment on the part of U.S. civilian and military leaders that unnecessarily delayed that defeat.

I have long admired Dr. Lambeth, a former RAND researcher with a long list of airpower-related writings, including in-depth examinations of airpower's role in conflicts such as Kosovo, Afghanistan, and the 2003 war in Iraq. Indeed, he has established himself as one of American airpower's leading chroniclers—and advocates—in the post-Vietnam era.

To make his case about the war against IS, Lambeth uses an enormous amount of publicly available official documentation, academic scholarship, as well as media reports and commentary. What makes his writing particularly interesting, however, are the scores of personal interviews he conducted along with emails he exchanged with participants—especially U.S. Air Force officers—about the operation, a style that has become something of his trademark.

Lambeth charts the transformation of American airpower in the years after Vietnam and points to "breakthrough developments in the realms of stealth, precision strike capability, and enhanced battlespace awareness"—all accompanied by better training and the development of fresh ideas about force application. Lambeth argues that despite success in Operation *Desert Storm* and Kosovo, airpower was too often underused and ill-used in post-9/11 counterinsurgency (COIN) fights in Iraq and Afghanistan and continuing for much of Operation *Inherent Resolve*.

Airpower in the War Against ISIS is not simply a history of events; it is an analysis of the policies and strategies that governed the campaign against IS. Many will find that analysis uncomfortable, as Lambeth does not hesitate to point fingers. For example, Lambeth traces the issues that manifested themselves in *Inherent Resolve* to the tenure of former Secretary of Defense Robert Gates. Though Gates was gone before the IS threat emerged, his disparagement of the Air Force as suffering from "next-war-itis"—that is, too much focus on possible conflicts with peer or near-peer competitors, such as China and Russia, instead of on the COIN conflicts—eroded what Lambeth argues was the "once orderly maturation of American air and space power."

This issue and other factors led to an "institutional identity crisis" for the Air Force, which in turn produced "a gradual but inexorable erosion" of thinking and planning skills that "had previously developed to a high art form toward making American airpower so decisive in previous tests of strength." Lambeth believes that the Air Force centered itself so much on the COIN fight that its skills to fight other types of adversaries atrophied. Furthermore, Lambeth argues that since 9/11, the leadership of U.S. Central Command (USCENTCOM), the organization responsible for the Middle East, had been overwhelmingly dominated by Army and Marine officers who did not fully grasp the warfighting potential of airpower. This excessively ground-centric orientation would persist into Operation *Inherent Resolve* to the campaign's detriment.

Lambeth finds that when the IS threat became impossible to ignore in 2014, the U.S. reaction, hobbled by political restraints, resulted in a "lethargic and directionless air effort." Moreover, Lambeth finds USCENTCOM's strategy to have been fundamentally flawed as the command applied a "planning template for winning indigenous hearts and minds in a COIN war to a totally different class of enemy that needed to be dealt with instead as a self-avowed state possessing territory, and infrastructure, and economy, a central nervous system, a targetable leadership, and the beginnings of a conventional army." Additionally, Lambeth contends the inappropriate COIN orientation resulted in what he characterizes as "counterproductive rules of engagement" (ROEs). Lambeth describes a highly restrictive ROE process that required convoluted coordination and vetting procedures that, among other things, demanded virtually no civilian casualties. More effective processes were implemented with a change of administration, eventually devastating IS.

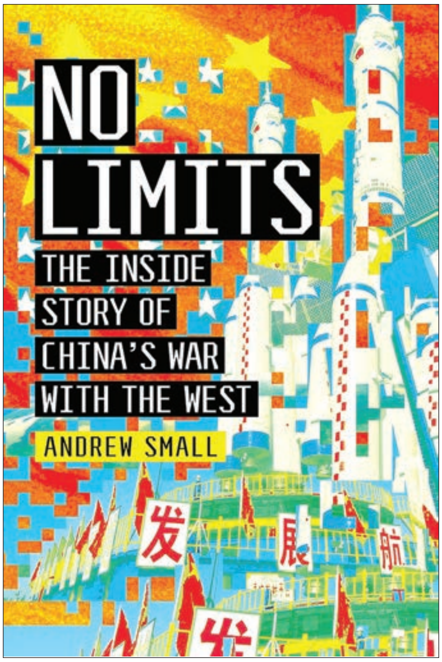
Lambeth makes clear that despite ultimately achieving success, "ill-advised leadership directives, in this case an inappropriate gradualist strategy at the campaign's start that misunderstood the enemy and wrongly insisted on ROE intended for a different kind of war," cost lives. He bluntly charges:

> [T]*here were the incalculable but monumental human costs that were imposed by the war's overly prolonged and pointless early incrementalism. Without seeking at this point to provide even a rough estimate of the number of innocent Iraqis and Syrians who were killed or wounded throughout the more than four-year-long campaign, the anemic start that President* [Barack] *Obama insisted on at the effort's outset and sustained with no truly consequential escalation for two more years produced millions of displaced civilians and caused a profusion of noncombatant fatalities in both countries, most of them at the hands of* [IS] *marauders rather than as the result of any errant coalition bombs.*

Lambeth's book is especially timely, as it comes as the Department of Defense is implementing its much-touted Civilian Harm Mitigation and Response Action Plan. This plan aims to institutionalize a bureaucracy with restrictive use-of-force policies that are disturbingly similar to that which proved so problematic in the air war against IS.

Airpower in the War Against ISIS stands for the proposition that airpower forcefully applied in a timely manner by savvy commanders will accomplish the mission with the least amount of civilian harm. It is a must-read not only for military professionals but also civilians wanting to understand how airpower could be optimally used in modern battlespaces. **JFQ**

Major General Charles J. Dunlap, Jr., USAF (Ret.), is Executive Director of the Center on Law, Ethics, and National Security at the Duke University School of Law.



No Limits: The Inside Story of China's War With the West (sold in Europe as The Rupture: China and the Global Race for the Future)

By Andrew Small
London: Melville House Publishing, 2022
288 pp. $29.99
ISBN: 978-1685890193

Reviewed by Thomas F. Lynch III

No Limits: The Inside Story of China's War With the West is a valuable book. It is simultaneously analytical and personal. *No Limits* is an incisive, selective history about how the promise of China's integration into Western economic systems and global institutions gave way to acrimony and rivalry. It also is author Andrew Small's memoir about how his quarter-century-long iterative interactions with China evolved from hope and cautious optimism about Sino-global integration into resigned fatalism that the Chinese Communist Party (CCP) can never tolerate such a happy ending. The CCP must instead view itself as perpetual victim and implacable rival of the West.

Small has unique personal expertise on the promise and peril of China. A native Brit, Small was an English teacher in a rural Chinese village in the late 1990s, then worked in the early 2000s as director of the Foreign Policy Centre's office in Beijing, at a time when the Western trade and banking sector was growing fast. He ultimately settled into his present, almost two-decade role as a senior transatlantic fellow with the Asia Program at the German Marshall Fund of the United States. Throughout this quarter-century studying Chinese relations with especially America and Europe, Small developed special and trusted relations with an array of prominent Chinese political, economic, and military figures. He also gained impressive professional understandings and unique personal insights that make his ringing of alarm bells in *No Limits* about the CCP's dangers to the Western-led international order resonate loudly.

Small tells us in *No Limits* that he felt the positive potential of China's rise. He knew many in Chinese economic and political leadership who saw the opportunity to export expanding national wealth and know-how to enhance growth in parts of the world left behind by Western economic organizations and development institutions. Small reminds us that China's outward face in the 1990s and early 2000s featured business-friendly personae like Premier Wen Jiabao (2003–2013) and Chairman of the Board of the China Investment Corporation—China's sovereign wealth and development fund—Jin Liqun (2008–2013). Small writes of how Wen, Jin, and others of that era soothed Europe and calmed America while smoothing pathways for Western businesses into China, stimulating Chinese economic demand and holding onto Western bonds and stocks during the tumultuous Great Recession in a manner that helped arrest global financial calamity. They then invested an enormous amount of China's wealth into the struggling economies of southern and eastern Europe, when richer European and American investments dried up.

But behind this early promise, Small reminds us of enduring peril. The CCP was there lurking—profiting from economic growth but paranoid about any challenge to its political strength or omnipotence. Historians often point to the Tiananmen Square protests and massacre of 1989 as the post-Mao benchmark of CCP limits on how much economic growth and openness could be tolerated in China. Small transports us to the 1999–2001 period for continuity in evidence that CCP strictures and constraints on political and economic activity could be relaxed a bit, but never forsaken, even in a fast-modernizing China.

He tells how in 1999 students from his rural former school were rounded up by CCP officials and trucked to a U.S. consulate for a CCP-choreographed protest of the accidental American bombing of the Chinese embassy in Belgrade days earlier. The students were paid and saw the demonstration as a field trip, but the incident demonstrated CCP reach, political authority, and control. Small then recounts how in 2001, China acceded to the World Trade Organization (WTO) at American and Western insistence but without Beijing's first having committed to WTO rules like constraint of government export subsidies, adherence to fair labor standards, or acceptance of environmental protections. This set the stage for decades of international economic damage.

Once China was in the WTO, CCP-run business and CCP-overseen private ventures set in motion a flood of Chinese state-subsidized, hypercompetitive exports. Abroad, these exports hit blue-collar legacy industries and workers exceptionally hard, increasing unemployment and driving cavernous income inequality in a manner that catalyzed ideological polarization in many countries. As China did not formally recognize the arbitration mechanisms of the WTO to be binding, the forum became less of a cooperative trade-expanding enterprise and more of a litigious assembly for growing unresolvable squabbles over trade practices seen as unassailable in the CCP's dogma of "capitalism with Chinese state characteristics."

Small's narrative reminds us that these early coal-mine canaries sang but were not heard. It took until much later—into the late 2010s—for Western leaders to recognize the ill-will borne them by CCP leaders. By then, Western-oriented, reform party leaders such as Wen Jiabao found themselves under scrutiny by CCP traditionalists for corruption. Wen himself vanished into isolation in the wake of a 2012 Party-led corruption investigation, and Small recounts how some of Wen's most trusted young advisors found themselves placed under house arrest or fled the country to avoid such a fate. A great firewall grew up around China's Internet, Party restrictions on semiprivate companies multiplied, and a crackdown on Hong Kong political protests ensued, as did a callous CCP refusal to accept any responsibility or accountability during the COVID-19 pandemic. In this saga of a resurgent, liberty-strangling CCP, the rise of Xi Jinping might have been an accelerant, but the campfire already was burning. America and Europe were slow to accept that an unchastened CCP was doing again what it always had done: whatever it needed to do at whatever cost to retain control. As Small observes sagely, but ruefully:

> *the longstanding* [Western] *push to embrace and integrate China was characterized in part by the hope that since its ambitions for wealth, influence and power were realizable within the system, the Chinese Communist Party could accommodate itself to it and that some of the other faces of China would still be part of that process. Understandably, there has been a great reluctance to give up on that bet.*

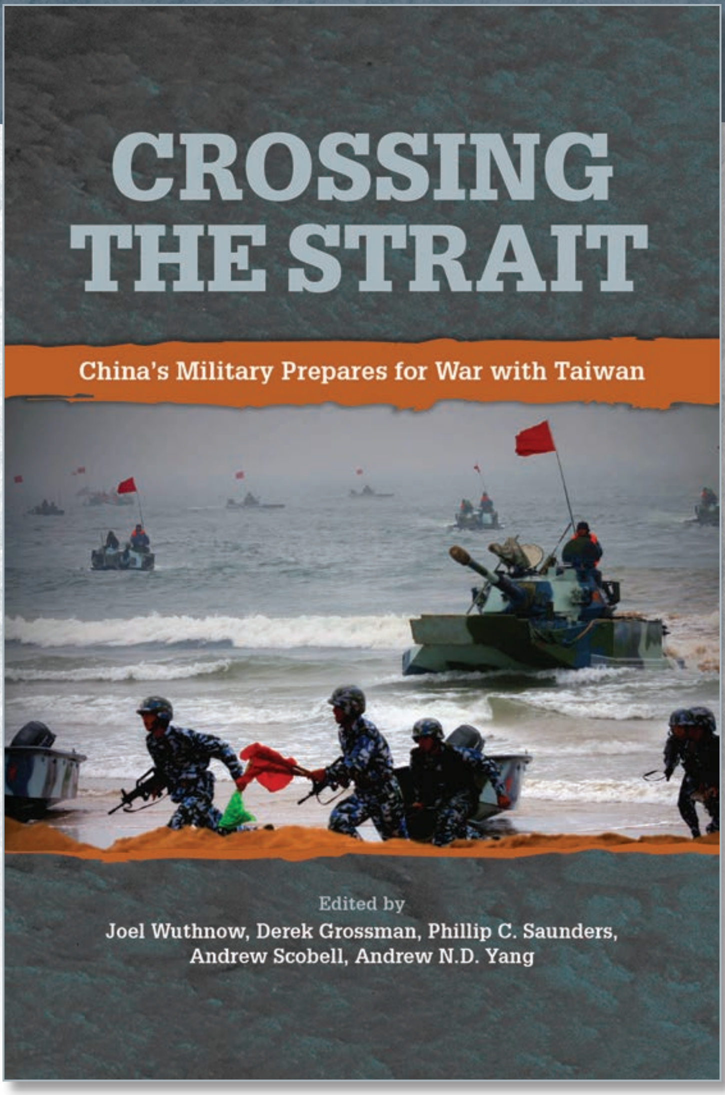
Small's warning in *No Limits* is a clarion call. The promise of liberalization and democratization is impossible under the CCP. In this conclusion, Small aligns with those found in recent works like Aaron Friedberg's *Getting China Wrong* (Polity, 2022), Rush Doshi's *The Long Game: China's Grand Strategy to Displace American Order* (Oxford University Press, 2021), and Hal Brands and Michael Beckley's *Danger Zone: The Coming Conflict With China* (Norton, 2022), among others. But as Small lived the decline of Chinese promise personally, his warning to American and European senior figures should carry extra weight. The negative rethink on China dominant today was not driven by hostile know-nothings who wanted to see Beijing fail, but by many of those who had been closest to China and wanted to see China succeed. Like Small, they now view China as a scary place and the CCP as a determined and dangerous global adversary.

Small warns that Western success can be secured only if the West's leaders now focus like a laser on this implacable and determined rival. By extension, joint force leaders must prioritize the growing Chinese military as the pacing, near-peer threat. They must innovate, organize, and train the joint force primarily to counter a CCP-led China that the October 2022 U.S. National Security Strategy identifies as the only country with both the intent to reshape the American-led international order and, increasingly, the power to achieve it. **JFQ**

Dr. Thomas F. Lynch III is a Distinguished Research Fellow in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.

From NDU Press

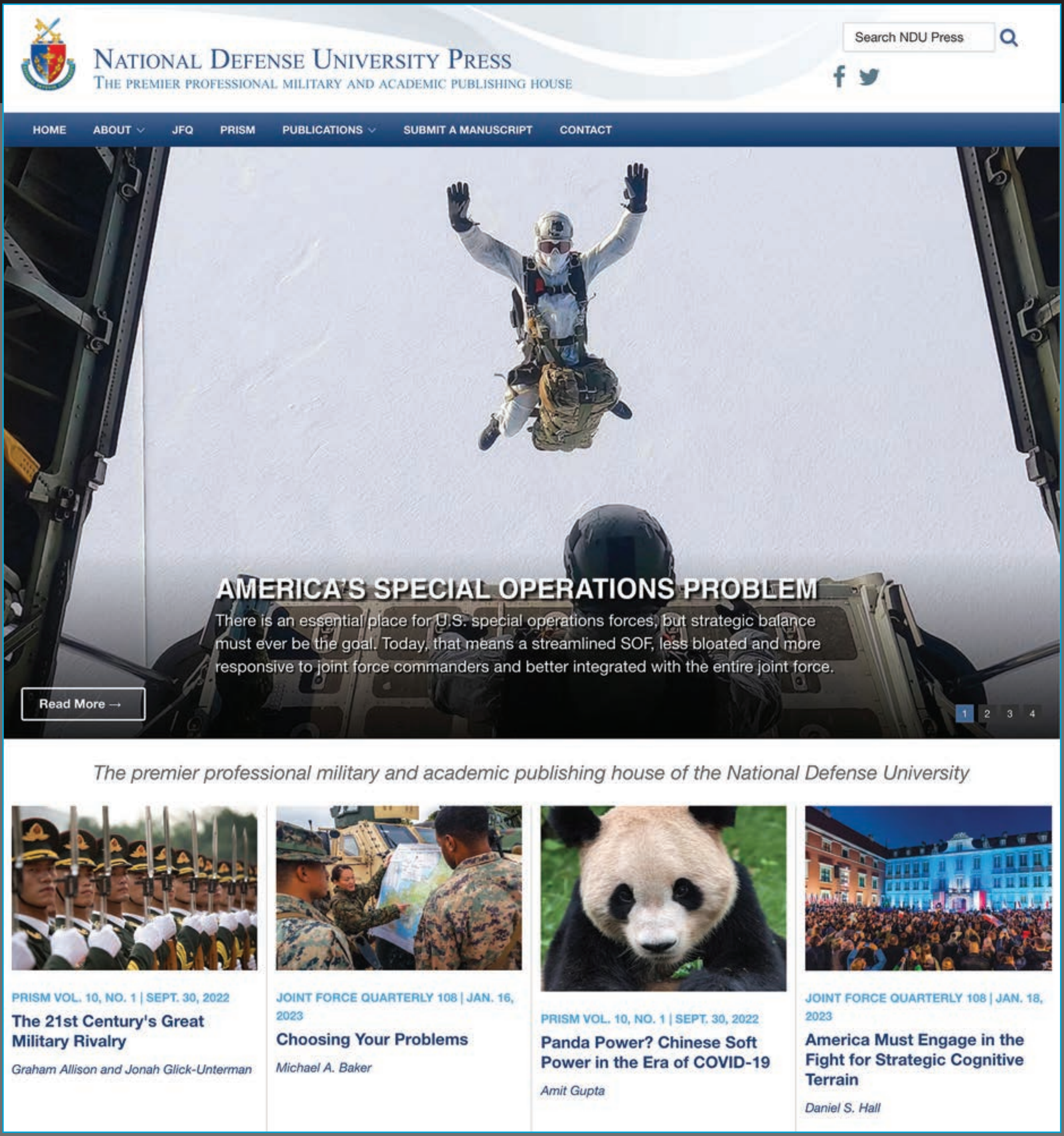
for the Center for the Study of Chinese Military Affairs


CROSSING THE STRAIT
China's Military Prepares for War with Taiwan
Edited by
Joel Wuthnow, Derek Grossman, Phillip C. Saunders,
Andrew Scobell, Andrew N.D. Yang

Both the U.S. and Chinese militaries are increasingly focused on a possible confrontation over Taiwan. China regards the island as an integral part of its territory and is building military capabilities to deter Taiwan independence and compel Taiwan to accept unification. Based on original research by leading international experts, *Crossing the Strait: China's Military Prepares for War with Taiwan* explores the political and military context of cross-strait relations, with a focus on understanding the Chinese decision calculus about using force, the capabilities the People's Liberation Army would bring to the fight, and what Taiwan can do to defend itself.

Check Out NDU Press Online!

Each year more than 1.5 million people visit the NDU Press Web site from around the world to discover the issues the joint force is experiencing in current policy, security, and warfighting arenas.



National Defense University Press
The premier professional military and academic publishing house

AMERICA'S SPECIAL OPERATIONS PROBLEM

There is an essential place for U.S. special operations forces, but strategic balance must ever be the goal. Today, that means a streamlined SOF, less bloated and more responsive to joint force commanders and better integrated with the entire joint force.

The premier professional military and academic publishing house of the National Defense University

PRISM VOL. 10, NO. 1 | SEPT. 30, 2022
The 21st Century's Great Military Rivalry
Graham Allison and Jonah Glick-Unterman

JOINT FORCE QUARTERLY 108 | JAN. 16, 2023
Choosing Your Problems
Michael A. Baker

PRISM VOL. 10, NO. 1 | SEPT. 30, 2022
Panda Power? Chinese Soft Power in the Era of COVID-19
Amit Gupta

JOINT FORCE QUARTERLY 108 | JAN. 18, 2023
America Must Engage in the Fight for Strategic Cognitive Terrain
Daniel S. Hall

You can also find us on:

X

Facebook

JFQ
JOINT FORCE QUARTERLY
Published for the Chairman of the Joint Chiefs of Staff by National Defense University Press
National Defense University, Washington, DC

NDU Press