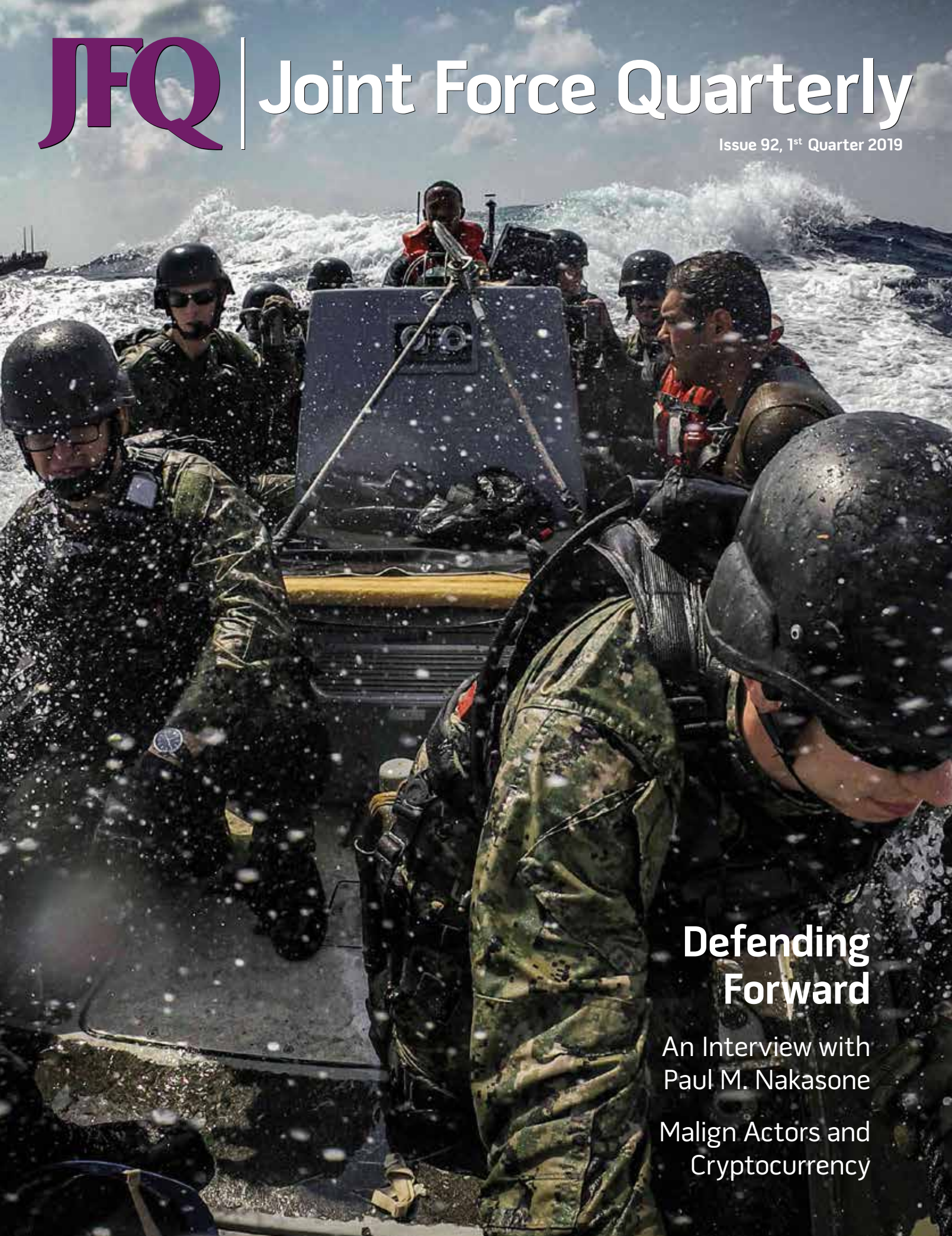
JFQ | Joint Force Quarterly

Issue 92, 1st Quarter 2019



Defending Forward

An Interview with Paul M. Nakasone

Malign Actors and Cryptocurrency

Joint Force Quarterly

Founded in 1993 • Vol. 92, 1st Quarter 2019

http://ndupress.ndu.edu

Cover 2 images (top to bottom): Staff Sergeant Levi McGowan, assigned to Bravo Company, 299 Brigade Engineer Battalion, 1st Stryker Brigade Combat Team, 4th Infantry Division, jumps to reach end of obstacle during Best Sapper Competition, Fort Carson, Colorado, November 2018 (U.S. Army/Asa Bingham); U.S. Marines attending Corporal's Course on Marine Corps Base Hawaii low crawl on Fort Hase Beach during Small Unit Leadership Evaluation, December 2018 (U.S. Marine Corps/Jesus Sepulveda Torres); U.S. Airman with 386th Air Expeditionary Wing participates in Explosive Ordnance Disposal Memorial Challenge in Southwest Asia, May 2015 (U.S. Air Force/Brittany E. Jones)

In This Issue

About the Cover
Sailors maneuver rigid-hull inflatable boat alongside USS *Carney* while training in Mediterranean Sea during U.S. Central Command exercise Bright Star 2018, held with Arab Republic of Egypt, September 10, 2018 (U.S. Navy/Ryan U. Kledzik)

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
260 Fifth Avenue (Building 64, Room 2504)
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 2019
ISSN 1070-0692

President Barack Obama meets with President George H.W. Bush in Oval Office, February 15, 2011 (The White House/Pete Souza)

Executive Summary

Those of us who have served in our nation's uniform have a common and permanent bond to our nation and to service to others. We may get caught up in the seemingly overwhelming day-to-day tasks of life, but the longer we serve, the tighter the bonds of military service hold us together. Older citizens may remember a time when military service was not honored as it is today. As a society, Americans now separate the value of an individual's military service from the debate over how the military is used to further national interest. One need only visit one of our nation's national cemeteries to get a fuller appreciation of the breadth and depth of American military service since the Revolutionary War. One cannot help but feel the weight of history and the price paid for what we enjoy as a society today.

Two recent events helped remind me of how military service forms a central reinforcing part of our nation: the loss of two American giants of national and military service, Senator John McCain and President George H.W. Bush, and the nationwide nonprofit effort "Wreaths Across America," which is supported by volunteers who place holiday decorations at military graves across the county.

American citizens took pause twice in recent months to honor these two military heroes from different generations and wars with the passing of Senator McCain and President Bush. We were reminded of the service and sacrifice each endured over the course of their remarkable lives. We were given time to reflect on each one's contributions to our nation's defense and, later, how they served in the political arena to forward their visions of a better America and our place in the world. Even those who may have had political differences with these men and their supporters were brought together to honor their service and their passing. During the course of their lives, Senator McCain and President Bush showed remarkable courage and unfailing drive to give back all they could to the rest of us.

For the past few years, I have participated in the annual laying of holiday wreaths at Arlington National Cemetery. Some 60,000 volunteers came that rainy Saturday to help place some 65 tractor trailer–loads of wreaths. Rain may have limited the crowd but not the effort,

as it took only a few hours to complete the task. At every stop we made during that day, I contemplated the history and service of thousands of Servicemen and women and their loved ones documented on those stones. As I was leaving the grounds, I inadvertently ended up at President John F. Kennedy's memorial with its eternal flame. One cannot help but take a moment to consider what was or could have been. We have such a rich history as a nation. What a grand place to honor those who served for all of us. We will never know the full measure of their sacrifice, but all we have to do is look around in a sacred place such as Arlington National Cemetery to appreciate the value of service to the Nation. Lest we forget.

This issue's Forum opens with my interview with the commander of the newest combatant command, General Paul Nakasone, USA, of U.S. Cyber Command at Fort Meade, Maryland. The general and I discussed how he sees the command fulfilling its unique mission and the role his teams play in the joint force, the interagency community, and with our international partners. Focusing on dealing with the range of virtual threats the United States faces, General Nakasone believes his command now has the right people, technology, and, most importantly, the right policy guidance to deliver on its assigned mission. Expanding on the themes we discussed, General Nakasone provides a compressive look at the threats, activities, and joint operations the command is working. Continuing to help us understand the complexity of cyber warfare, Frank Sanchez, Weilun Lin, and Kent Korunka offer us a discussion of how the principles of irregular warfare inform how we might address conflict in this newest medium.

As our JPME Today section returns, we offer the first of what will be a number of articles in response to the latest call, in the 2018 National Defense Strategy by Secretary James Mattis, to reform professional military education. Colleagues at the Joint Forces Staff College (JFSC), Chuck Davis and Fred Kienle, writing with a frontline JPME perspective, believe the best way to meet the Secretary's challenge is to focus on the original purpose of JPME Phase II programs as provided in the Goldwater-Nichols Department of Defense Reorganization Act of 1986. While on Active duty, Colonel Kienle was the leader with the insight and drive to successfully develop, execute, and lead the Joint Advanced Warfighting School (JAWS) program at JFSC, where JAWS continues to graduate world-class "Jedi" joint planners for the combatant commands, the interagency community, and international partners. Our joint force owes him a great deal for his long service to JPME. Next, returning *JFQ* author and center of gravity expert Dale Eikmeier describes how simplicity can be employed to come up with effective solutions to a planner's more difficult problems.

We have a pair of thought-provoking articles in this edition's Commentary. Since serving on a combatant command staff provides one with a valuable perspective on how these commands are able to deal with 21st-century challenges, John Fawcett tips his hat to the Napoleonic-era staff model still in use today as he recommends some structural changes needed to finally bury the emperor's legacy and organize our joint operations better. Jeffrey Zust and Stephen Krauss provide their insights on how to best help our joint force leaders protect their people from the invisible wounds of conflict.

The Features section offers interesting and useful ideas about a range of issues. First, Neil Hollenbeck, Arnel David, and Benjamin Jensen present their take on the age-old discussion of how business principles might offer some important tools for warfighting. Next, Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden team up to give us their expert views on how the joint force should be prepared to follow the money that threat groups use to fund their operations in a completely new way, through the use of virtual cash or cryptocurrency. As U.S. forces are employed more sparingly in areas of conflict through strategies such as "by, with, and through," Jahara Matisek and William Reno discuss the political aspects program managers and field leaders need to understand for the effective deployment of security force assistance programs.

Our Recall article takes us back to a dark chapter of air and land operations—the 1943 debacle at Kasserine Pass in North Africa—where Leland Cowie helps us see how to best employ joint air in the 21st century.

In Joint Doctrine, Matthew Quintero welds together three different domain-based but synergistic concepts to recommend important new ways to achieve success in joint air operations. After 17 years of insurgency-focused warfare, the update of Joint Publication 3-24, *Counterinsurgency*, should provide readers with much to consider going forward, and we have a brief article discussing this new version. We also have four useful reviews on a range of books for you to consider reading, and, as always, the Joint Staff's Joint Doctrine Update on where other joint publications are in the review process.

As the year closes, we tend to look both backward and forward. Each of us draws on the past to help guide us in the future. Please take the time to remember those who have served and those who are serving. Submit an article that will help the future joint force learn from your experience of service and sacrifice. When you have that lesson down, send it to us so we can pass it along. JFQ

William T. Eliason
Editor in Chief

An Interview with Paul M. Nakasone

JFQ: *How do you view cyberspace in relation to the world that the joint force operates in? How is operating in cyberspace different from other warfighting domains?*

General Nakasone: As we think about cyberspace, we should agree on a few foundational concepts. First, our nation is in constant contact with its adversaries; we're not waiting for adversaries to come to us. Our adversaries understand this, and they are always working to improve that contact. Second, our security is challenged in cyberspace. We have to actively defend; we have to conduct reconnaissance; we have to understand where our adversary is and his capabilities; and we have to understand their intent. Third, superiority in cyberspace is temporary; we may achieve it for a period of time, but it's ephemeral. That's why we must operate continuously to seize and maintain the initiative in the face of persistent threats. Why do the threats persist in cyberspace? They persist because the barriers to entry are low and the capabilities are rapidly available and can be easily repurposed. Fourth, in this domain, the advantage favors those who have initiative. If we want to have an advantage in cyberspace, we have to actively work to either improve our defenses, create new accesses, or upgrade our capabilities. This is a domain that requires constant action because we're going to get reactions from our adversary. From that reaction stems our next move.

Unlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the *use* of cyber capabilities that is strategically consequential. The *threat* of using something in cyberspace is not as powerful as *actually* using it because that's what our adversaries are doing to us. They are actively in our network communications, attempting to steal data and impact our weapons systems. So advantage is gained by those who maintain a continual state of action.

In the last 10 years, our adversaries have been operating below the threshold of armed conflict, stealing our intellectual property, leveraging our personally identifiable information, or attempting to influence our elections—again, all below the threshold of armed conflict. We have seen our adversaries conduct these strategic campaigns where a series of tactical actions allow our adversaries to have strategic impact by degrading our sources of national power. This is why U.S. Cyber Command [USCYBERCOM] evolved its strategic concept and operational

General Paul M. Nakasone, USA, is Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service.

approach from a response force to a persistence force, as I explain in my follow-on article in this issue of *JFQ.*

JFQ: *How big is the threat matrix that your command faces? What is the relationship between what your command can do to deter, defend, and defeat adversaries, and what you must rely on other entities to do for cyber defense?*

General Nakasone: Let's take a step back and think about what the threats are to our nation. Ten years ago, threats were primarily other nations trying to exploit us. They were trying to get into our classified systems, steal our information. This is what we consider espionage. There was a period of time where we were concerned primarily about foreign intelligence services coming into our networks and stealing information. That rapidly changed after 2013 when states began disrupting a series of networks within the United States. In 2012–2013, the distributed denial-of-service attacks conducted by the Iranians against the financial networks in New York changed our calculus. These were *disruptive* attacks. So we moved from exploitation to disruption. And by 2014, we saw *destructive* attacks. We witnessed the Iranians in February 2014 conduct a data deletion attack against an American casino. And then in November, Sony Pictures was attacked by the North Koreans. So in a period of 10 years, nation-states progressed from exploitation, to disruption, and finally to destructive attacks against us in cyberspace.

But now we're seeing what many call a *corrosive* threat, which is the ability to weaponize information in order to conduct influence campaigns, steal intellectual property, or leverage someone's personally identifiable information. We've seen our adversaries doing this in places like Iraq, Syria, Ukraine, the 2016 elections, and the hack of the Office of Personnel Management. The question then becomes, "What does a state do to defend against that?"

Thus far, our responses against adversaries who have penetrated our networks or stolen our data or defaced our Web sites have not worked. We've learned that if we're going to have an impact on an adversary, we have to *persistently engage* with that adversary, we have to understand that adversary, we have to be able to impose cumulative costs on that adversary, and we have to be able to understand where that adversary not only is but also where he is going.

JFQ: *A number of years ago, the original concept of having a cyber command was primarily defensive in nature because offensive operations were really not what we are about. But I think the more the public understands about cyber, the more they think we can't just sit back and take punches. How does U.S. Cyber Command see this issue?*

General Nakasone: The Department of Defense [DOD] has an important role to play in the defense of the Nation in cyberspace. We enable both the Department of Homeland Security [DHS] and Federal Bureau of Investigation [FBI] with information and intelligence to more effectively work with the private sector. USCYBERCOM has developed strong partnerships with DHS, the FBI, and sector-specific agencies for select critical infrastructure and key resource sectors. We are doing this purposefully, in partnership with DHS and private-sector leads. It is critical that we develop these partnerships prior to a possible crisis.

JFQ: *We have heard a great deal about Russian interference and misinformation in the U.S. election process, which you noted a moment ago. What other problems are you concerned about from the Chairman's "2+2+1" challenges: Russia and China, Iran and North Korea, and violent extremist organizations? How do they compare to each other, and how are the responses different?*

General Nakasone: I think it is wise, as we look at the alignment of threats, to realize that we're in a period of great power competition. The National Security and National Defense strategies clearly stated that over the past 10 years, any advantages that we had—to include in cyberspace—have eroded as our adversaries have caught up. As we look at near-peer competitors, China and Russia clearly are at the top of the list because they have capacity to operate across the full spectrum of cyberspace operations. Behind China and Russia are the Iranians and North Koreans, who are unique in demonstrating both capability and intent to strike us in cyberspace. We pursue varying strategies to address all four of these nation-states. Additionally, as we have learned in combating [the so-called Islamic State] in cyberspace, we must maintain visibility on nonnation state adversaries as well in this domain.

JFQ: *Cyberspace is now a growing security industry dedicated to find and neutralize state and private cyber attackers and tools. How is this affecting military operations? Is your command able to deal with the weaponization of information? How does that fit in the more conventional military role of operations?*

General Nakasone: The National Defense Strategy outlines that partnerships are one of the three key elements we must possess to compliment and enhance our warfighting capabilities. Partnerships are fundamentally something that we must do in cyberspace. In fact, one of our priorities is to build strong, reliable, and resilient partnerships because this is a domain where 90 percent of the networks—the critical infrastructure—resides in the private sector, not in the public. This is primarily a private industry-driven domain.

Think of the antivirus community and how it has grown in the last few years. What do they have? They have global presence, and the ability to collect an enormous amount of information. They have strong analytic capabilities. The products they produce often rival what we see being done by the Intelligence Community. These partnerships—and particularly with private industry—are

Cyber warfare operators serving with 175th Cyberspace Operations Group of Maryland Air National Guard monitor cyber attacks on operations floor of 275th Cyber Operations Squadron known as Hunter's Den, December 2, 2017 (U.S. Air Force/J.M. Eddins, Jr.)

critical for what we're doing in cyberspace today. We have a number of different initiatives that are reaching out to the private sector because we know that a lot of the cutting-edge technology that's being used today in cyberspace resides within private industry.

JFQ: *How difficult is it for the military to compete with the private sector?*

General Nakasone: This is a common question—a good question given the competition for talent across government, private industry, and acadamia. We think of this competition across the recruitment, training, and retention of a force. In recruitment, the Services do a tremendous job of attracting young men and women to join our teams. Why do the Services get top talent? Because young people want to join and do this type of work. Second, we have a strong training program. In fact, it is so good that not only do we train them, but we also have the opportunity to earmark those who are the top talents. Once we have earmarked the top talent, then the question becomes, "How do we retain them?" The retention problem is not a macro problem—we have proved we can retain the overall numbers of Servicemembers to maintain our force. The challenge is ensuring we retain our very best. Those very best are often exponentially better than their peers—10 or 20 times better. They're coders, they're forensic and malware analysts, they're developers, they're operators who are *x* times better than those to their left or right. Those are the folks we must ensure we retain. They are the ones we are in fierce competition to keep.

JFQ: *You've spoken in other forums about the concept of "persistent engagement" and even mentioned it earlier. In relation to your mission, can you describe what you mean by that phrase and how it relates to the National Defense Strategy?*

General Nakasone: *Persistent engagement* is the concept that states we are in constant contact with our adversaries in cyberspace, and success is determined by how we *enable* and *act*. In persistent engagement, we *enable* other interagency partners. Whether it's the FBI or DHS, we enable them with information or intelligence to share with elements of the CIKR [critical infrastructure and key resources] or with select private-sector companies. The recent midterm elections is an example of how we enabled our partners. As part of the Russia Small Group, USCYBERCOM and the National Security Agency [NSA] enabled the FBI and DHS to prevent interference and influence operations aimed at our political processes. Enabling our partners is two-thirds of persistent engagement. The other third rests with our ability to act—that is, how we act against our adversaries

in cyberspace. Acting includes defending forward. How do we warn, how do we influence our adversaries, how do we position ourselves in case we have to achieve outcomes in the future? Acting is the concept of operating outside our borders, being outside our networks, to ensure that we understand what our adversaries are doing. If we find ourselves defending inside our own networks, we have lost the initiative and the advantage.

JFQ: *When I was interviewing Admiral* [Michael] *Rogers, he was in the process of building teams to stand in the early days of cyber. How is your progress in getting to where you want to be to have all your teams in place to accomplish your mission?*

General Nakasone: One hundred thirty-three teams are built and trained to a joint standard, and that is complete. Our focus has gone from building teams to making sure they're *ready* teams, making sure the teams, whether offensive or defensive, have the capabilities, have the manning, have the tradecraft, have the experience to conduct the missions that I talked about earlier. It's our primary focus. One of the things that we have going for us is that we have some pretty active adversaries. Whether it's countering adversaries who are trying to impact our elections; whether it's opposing adversaries in places such as Iraq, Syria, Yemen, or Afghanistan; or whether it's working to ensure that our defensive teams are assisting in the protection of our weapon systems—we are ready.

JFQ: *U.S. Cyber Command is a relatively new organization, even in its recent elevation to command status. How have the capacity and capability of the command grown over time to meet your missions? Has jointness been a benefit to how the command operates?*

General Nakasone: Jointness has been a tremendous benefit to our cyber mission forces. In the early days of USCYBERCOM, the leaders decided on an important point: there would be only one training standard, a joint training standard determined by USCYBERCOM. That's helpful for any commander who gets a Marine team, Army team, Navy team, or Air Force team and knows that whatever Service team he receives, missions will be executed to a single joint standard. We have a number of different missions with a number of different elements, so jointness is essential for us.

Looking back on the development of the force, there's been a series of different acts in the history of the command. Act 1, was standing up the command in May of 2010. Act 2, in 2012–2013, was the decision by DOD to build 133 teams—6,187 people (both military and civilian)—for 4 years in order to build capacity and capability across this command. Act 3 was the employment of these teams, both with Joint Task Force Ares, focused on the defeat of the [so-called Islamic State] in virtual space, and the recent Russia Small Group, which was a USCYBERCOM/NSA partnership to assist in the securing of the 2018 midterm elections. Across all these activites or acts, the concept of jointness has been fundamental to our thinking and our success.

JFQ: *How do you leverage partnerships at home, and internationally, to the command's benefit? What is your relationship to the various other places you may have forces, or how are you related to other commands globally?*

General Nakasone: When we take a look at our partnerships with other commands, we begin with geographic combatant commands. These are easy partnerships that we formed immediately. There's a known threat: there are known challenges to their networks, data, and the way they do business. We have also been the beneficiary of the DOD desire to stand up cyberspace operationally integrated planning elements. These elements are personnel who have cyber experience, who have gone to the commands to work within the J3 and J5 shops to provide the planning and subject matter expertise that was necessary. Moreover, we've been the beneficiary of ongoing operations in northern Iraq, Syria, Afghanistan, the Philippines, and Yemen to perfect a lot of our tradecraft with these supported commands. Then there are the functional or global commands. I appreciate both U.S. Special Operations and U.S. Strategic commands for pulling USCYBERCOM in and saying, "We are global commands, we need to think about this differently. We have shared areas that we have an ability to provide greater support to the Nation." That's appreciation for access and appreciation for a wide range of options. These are things that we among the [global commands] started talking about, and I think this would be among the big steps that USCYBERCOM and other commands will be able to offer the Nation in the years to come.

JFQ: *As these threats and responses evolve, what is your view of the long-term conflict in cyberspace? What changes in operational structures and technology do you think are necessary?*

General Nakasone: As we look to the future of competition in cyberspace, one idea comes to mind. The concept of persistent engagement has to be teamed with "persistent presence" and "persistent innovation." Persistent presence is what the Intelligence Community is able to provide us to better understand and track our adversaries in cyberspace. The other piece is persistent innovation. In the last couple of years, we have learned that capabilities rapidly change; accesses are tenuous; and tools, techniques, and tradecraft must evolve to keep pace with our adversaries. We rely on operational structures that are enabled with the rapid development of capabilities. Let me offer an example regarding the need for rapid change in technologies. Compare the air and cyberspace domains. Weapons like JDAMs [Joint Direct Attack Munitions] are an important armament for air operations. How long are those JDAMs good for? Perhaps 5, 10, or 15 years, sometimes longer given the adversary. When

More than 800 Servicemembers and civilians enhance readiness during Exercise Cyber Shield 18 at Camp Atterbury, Indiana, May 2018 (Indiana National Guard/Jeremiah Runser)

we buy a capability or tool for cyberspace . . . we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years. This is a big difference in two important domains of future conflict. Thus, we will need formations that have ready access to developers. Also, developers who understand how to complement the work of our operators in a rapid, agile manner.

JFQ: *I imagine your loop for acquisition has to be almost infinitely fast, lightspeed somewhat, say, compared to trying to develop an F-35 or some other kind of conventional or traditional system.*

General Nakasone: We have created programs for building capabilities in cyberspace. However, to your point, one of the very helpful things is that we have some acquisition authorities, and we have acquisition money that we are able to touch, so we've started doing that. The construct of operating and rapidly developing in tandem within this domain is one of the areas that makes this domain unique. Operators must work closely with developers, and the developers must work in partnership with our operators.

JFQ: *Obviously when U.S. Special Operations Command* [USSOCOM] *was set up under Goldwater-Nichols, it got a certain chunk of authority under Title 10 that the other commands do not have. In the future, do you foresee a need for asking for that kind of capability for U.S. Cyber Command since you're somewhat different than the other kinds of commands?*

General Nakasone: We are still at the point of building our infrastructure and capabilities and the development of networks, but once that's done, I think we will look for increased USSOCOM-like authorities. What underwrites success in cyberspace is the need for speed and agility. This will likely lead us to evaluate those authorities—whether it is in acquisition, joint force training, or joint force provision—that ensure we can operate rapidly with unmatched lethality.

JFQ: *What is artificial intelligence* [AI] *and what does it mean for the future of conflict in general and for the future of cyber security in particular?*

General Nakasone: When we talk about cyberspace, I think that the early instantiation of AI will be on the defensive side. We are experimenting and developing "self-healing networks," where we see a vulnerability and the vulnerability is recognized rapidly and patched or mitigated.

Yet AI will likely be part of future offensive capabilities as well. Currently, access development is our most time-consuming and difficult element of developing offensive options. I suspect that AI will play a future role in helping us discern vulernabilities quicker and allow us to focus on options that will have a higher likelihood of success.

JFQ: *I'll leave you some space for things that you think we may have not covered here and that you think are important to talk about. We touched just briefly on jointness. How have you seen jointness come to develop itself and where do you see it going from here? Not necessarily specific to U.S. Cyber Command, but as a member of the elite within the joint world, what does jointness mean to you as a commander?*

General Nakasone: I was commissioned in 1986, so my experience with jointness has taken place over the last 20 years. I have seen first hand the advantages of joint formations—whether it's been in combat or stateside. I operate comfortably within the joint world given several tours with the Joint Staff or within joint commands. It's natural for me to understand how to do joint planning processes. I believe USCYBERCOM has benefited tremendously from a joint construct. We operate as a joint force *habitually.* We will be even more joint in the coming 5 years given the power of being able to bring a "best athlete" approach across the Services to a problem. When we evaluate problems, we do see specific Service advantages, but that advantage has to be teamed with capability and capacity that other Services can offer. I see bringing our best operators, developers, and analysts across Services to solve tough problems as a large part of what the future is going to hold for us. We will always have Service equities in terms of what we're going to defend and be able to do, but increasingly our networks will be joint. Our training is moving much more toward a joint flavor than a specific Service flavor. USCYBERCOM in many ways will be at the cutting edge of this new and important movement toward jointness.

Venetian resort hotel casino, owned by Las Vegas Sands Corporation, was hit by Iranian cyber attack in February 2014 (Courtesy Bert Kaufmann)

JFQ: *Your teams are made up just as Service teams, or . . . ?*

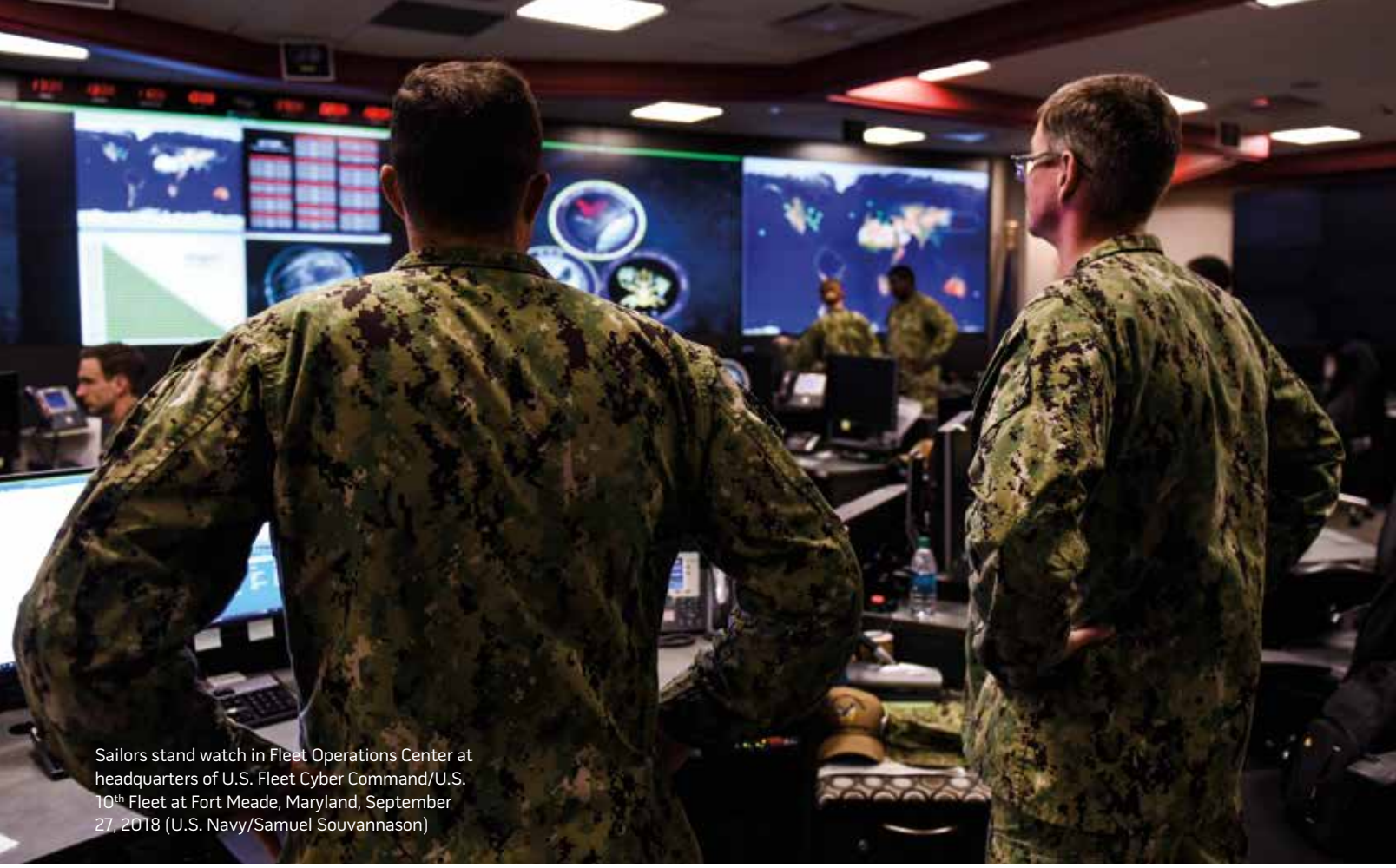
General Nakasone: The Services man, train, and equip our teams, but we operate regularly as part of joint task forces. This includes our major operations supporting the defeat [so-called Islamic State] campaign and the recent efforts to secure the midterm elections.

JFQ: *What is your greatest challenge?*

General Nakasone: Our greatest challenge—also our greatest opportunity—is recruiting, training, and retaining a world-class force. The Services continue to recruit high-caliber military and civilian personnel to man our force. We have developed a training pipeline that trains all to a common, joint standard. Our retention of top talent is a critical component of future success. We track this closely and work with the Services to identify opporutnities to improve retention. We must continue to build our recruiting and training successes along with a strong focus on ensuring we retain our best military and civilian personnel. The competition for talent is not getting any easier.

JFQ: *Thank you so much for your time.*

General Nakasone: Let me add one final point. We have a tremendous amount of momentum to build on in the coming months. The guidance resident in the National Security Strategy, National Defense Strategy, National Intelligence Strategy, National Military Strategy, National Cyber Strategy, DOD Cyber Strategy, and DOD Cyber Posture Review give us a clear vector to move us forward. This, coupled with clear policy guidance and the 2019 National Defense Authorization Act, ensure USCYBERCOM can operate at the speed of relevance to effectively accomplish its mission and bring greater capacity and capabilities to DOD and the Nation. **JFQ**



Sailors stand watch in Fleet Operations Center at headquarters of U.S. Fleet Cyber Command/U.S. 10th Fleet at Fort Meade, Maryland, September 27, 2018 (U.S. Navy/Samuel Souvannason)

A Cyber Force for Persistent Operations

By Paul M. Nakasone

Harvard's Samuel Huntington, then just 27, asked the U.S. Navy in 1954, "What function do you perform which obligates society to assume responsibility for your maintenance?" His seminal article in the U.S. Naval Institute's *Proceedings* argued that the basis of a military Service—or any military element—is its purpose or role in implementing national policy. Huntington called this a Service's "strategic concept," which justifies public support by explaining how, when, and where that military arm expects to protect the Nation.[1]

Huntington's question resonated because the Navy faced a crisis of purpose after World War II. It had helped win the biggest conflict in history, but the Allied victory over the Axis powers was so sweeping that by 1954 the Navy had no viable rivals left to fight at sea. The Navy's longstanding strategic concept as the Nation's first line of defense no longer seemed compelling. In addition, the prospect of nuclear war had shaken strategic assumptions and was reshaping American foreign and defense policies. While no enemies could reach America's shores from the oceans, one adversary—the Soviet Union—could devastate the country from the skies with hydrogen bombs. The Navy's traditional "oceanic" orientation, which had justified powerful fleets, seemingly had little relevance for the application of American power against nuclear-armed land powers in Eurasia.

The Navy subsequently developed a "transoceanic" strategic concept, orienting the Service away from contesting the oceans and toward projecting power across them to distant land masses. In adapting its strategic concept to reflect changes in threats and national policy, the Navy ensured public confidence and support from Congress. The Navy's new strategic role endured through the Cold War, helping the United States maintain the forces that contained Soviet power and ensuring that America (with its allies) was so strong at sea that Moscow never seriously contemplated building fleets to rival ours.[2]

General Paul M. Nakasone, USA, is Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service.

When our nation asks, "What function does U.S. Cyber Command (USCYBERCOM) perform that obligates society to assume responsibility for its maintenance?" the command can reply that its strategic concept has evolved from a "response force" to a "persistence force." This persistence force will contest our adversaries' efforts in cyberspace to harm Americans and American interests. It will degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace. Over time, a persistence force, operating at scale with U.S. and foreign partners, should raise the costs that our adversaries incur from hacking the United States. To protect our most critical public and private institutions from threats that continue to evolve in cyberspace, we cannot operate episodically.

While we cannot ignore vital cyber defense missions, we must take this fight to the enemy, just as we do in other aspects of conflict. A persistence force has a much higher chance of disrupting adversary plots and protecting Americans, compared with a force that is confined to sporadic reconnaissance. Persistence should not be mistaken for engagement for engagement's sake; instead, it is an approach that empowers U.S. cyber forces to achieve more decisive results in pursuit of objectives set by national leaders. This evolution aligns USCYBERCOM with changes in the strategic environment and in national policy as articulated in the 2017 National Security Strategy and 2018 National Defense Strategy.

Cyberspace and Great Power Competition

The growth of a global, interconnected cyberspace domain represents the biggest strategic development since 9/11. Activities and operations in, through, and from cyberspace now offer states the means to augment their power, degrade or usurp the power of others, and gain strategic advantage through competition *without triggering armed conflict*. Our adversaries have learned this and are leveraging it against us.

When cyberspace went global in the 1990s, its fundamentals seemed to align comfortably with Western values. For this reason, its acceleration of social interaction, economic exchange, scientific progress, and military operations proved troubling to dictators who worried that their hold on power would be undermined by digital-age capabilities empowering civil society. The Arab Spring in 2011 heightened these fears. In response, increasingly cyber-capable governments escalated their operations against their own citizens and ours. They mounted global surveillance of opposing views and are stealing unprecedented quantities of intellectual property and personal data, disrupting democratic processes, holding critical infrastructure at risk, and eroding U.S. power. They employ technical activities that are individually inconsequential, yet cumulatively set the conditions for decisive advantage in conflict should it occur.

The return of great power competition prompted the authors of the new National Security Strategy to lament that while Americans "took [their] political, economic, and military advantages for granted, other actors steadily implemented their long-term plans to challenge America and to advance agendas opposed to the United States, [its] allies, and our partners." Growing political, economic, and military competitions around the world, according to the National Defense Strategy, are now the central challenge to U.S. security and prosperity. In these competitions, the locus of struggle for power has shifted toward cyberspace, and from open conflict to competitions below the level of armed attack.

Original Concept

USCYBERCOM began operations in 2010 when exploitation and disruption comprised the major cyber threats to Department of Defense (DOD) information networks and the Nation's critical infrastructure. Even though the United States had enjoyed general superiority in cyberspace since the creation of the domain, our competitors had developed and acquired effective, if often rudimentary, capabilities as well. The command's mission was to maintain U.S. superiority by checking the capability development of our competitors. USCYBERCOM initially focused on defending DOD networks and supporting geographic combatant commanders, particularly in Iraq and Afghanistan. USCYBERCOM was thus a *response* force—executing counterterrorism operations, planning to support conventional forces in crisis scenarios, and maintaining capacity to respond to an "attack of significant consequence" against our critical infrastructure.

In 2013, a year that marked a strategic inflection point and the obsolescence of that original strategic concept, surprisingly capable adversaries now operated continuously against critical infrastructure, government networks, defense industries, and academia—both in America and abroad. Cyber-enabled intellectual property theft had long been common, but now state-sponsored malicious activities began to impose significant costs on the Federal Government and private sector. The adversaries mounting these campaigns took care to operate in ways that would not trigger an armed U.S. response. Examples of their assaults included the Iranian denial-of-service attacks against the financial sector (2012–2013) and attack on the Sands Casino (2014), North Korea's attack on Sony Pictures Entertainment (2014), and China's disruption of GitHub (2015) and theft of security-related data from the Office of Personnel Management (2015). Russia raised cyberspace campaigns to a new level of boldness after 2015, launching a series of operations to interfere with the elections of the United States and its allies and sponsoring attacks on the Ukrainian power grid. These campaigns convinced even skeptics that cyberspace activities over time could cumulatively erode a country's sources of national power.

Today peer- and near-peer competitors operate continuously against us in cyberspace. These activities are not isolated hacks or incidents, but strategic campaigns. Cyberspace provides our adversaries with new ways to mount continuous, nonviolent operations that produce cumulative, strategic impacts by eroding U.S. military, economic, and political power without reaching a threshold

that triggers an armed response. In other words, shifts in the global distribution of power can now occur without armed conflict. Hence the strategic concept of a response force—in effect, holding U.S. cyber forces in reserve for kinetic conflicts or responding after-the-fact to cyber attacks on America—resembles the Navy's pre-1945 strategic concept that Huntington critiqued. Worse still, it has had the effect of ceding the strategic initiative in cyberspace to adversaries willing to operate continuously against us. Continuous action in cyberspace for strategic effect has become the norm, and thus the command requires a new strategic concept.

A Cyber Persistence Force

We are learning how cyber capabilities can be employed to advance what the 2018 National Defense Strategy calls our "competition and wartime missions." Our adversaries are learning too, integrating and employing cyberspace capabilities in different ways consistent with their doctrine, strategy, organizational culture, and risk tolerance. History cautions that we should expect the use of new capabilities to evolve as they are introduced in conflicts. Tanks, for instance, developed from infantry support to deep penetration roles, while aircraft progressed from tactical reconnaissance to strategic bombing to unmanned intelligence, surveillance, and reconnaissance. With battlefield experience comes the evolution and maturation of operational concepts and strategic insights. Carl von Clausewitz noted that the "knowledge basic to the art of war is empirical," meaning theory must conform to experience.[3] USCYBERCOM has learned that successful engagement against adversaries in cyberspace requires that we continuously seek tactical, operational, and strategic initiative. Such persistence requires that we remain ahead of them both in knowledge and in action. It also demands that we leverage our strengths across intelligence and operations to achieve this end.

In March 2018, USCYBERCOM's command vision document, *Achieve and Maintain Cyberspace Superiority*, updated the command's strategic concept to align with changes in national strategy and in the cyberspace competition.[4] The document acknowledges that the locus of struggle in the revived great-power competition has shifted toward cyberspace and that decisive action can occur below the level of armed attack. Its strategic concept is "cyber persistence" rather than "cyber response," empowering USCYBERCOM to compete with and contest adversaries globally, continuously, and at scale, engaging more effectively in the strategic competition that is already under way.

USCYBERCOM's strategic thinking is evolving along with our forces and capabilities. We are accelerating change in the following ways:

- We are shifting our strategic perspective away from viewing war and territorial aggression as the only perils for our national sources of power. A byproduct of successfully deterring conventional and nuclear war is that adversaries now shape America's policy choices through cyberspace operations calibrated to avoid provoking armed responses. Because our adversaries still feel able to operate against the United States and its interests through cyberspace, and because historically there has been little cost imposed for doing so, USCYBERCOM must operate below traditional use-of-force thresholds while also preparing to be a lethal force in conflict.
- We are building relationships with U.S. institutions that are likely to be targets of foreign hacking campaigns—particularly in the Nation's critical infrastructure—before crises develop, replacing transactional relationships with continuous operational collaboration among other departments, agencies, and the private sector. These relationships are crucial to thwarting attackers before they strike and to increasing resilience after a successful breach. Ideally, these partnerships will allow our persistence force to address patterns of malicious cyber behavior before they become attacks.
- We must "defend forward" in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace. Persistent engagement of our adversaries in cyberspace cannot be successful if our actions are limited to DOD networks. To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well. Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment.
- We have shifted away from the earlier emphasis on holding targets "at risk" for operations at a time and place of our choosing. We will operate continuously to present our decisionmakers with up-to-date options. Cyberspace targets themselves typically amount to computer and data "states," which change constantly in the normal functioning of digital information systems. Successful operations require capabilities and tactics that can rapidly shift from unsuccessful approaches in order to exploit new vulnerabilities and opportunities.
- Finally, we are ensuring our capabilities, operational tempo, decisionmaking processes, and authorities enable continuous, persistent operations. Adversaries and competitors have responded to our restrained and episodic engagement with cyber aggression that has eroded U.S. military, economic, and diplomatic advantages. Strategic effects in cyberspace come from the use—not the mere possession—of cyber capabilities to gain the initiative over those who mean us harm.

Airmen gather around computer at first U.S. Air Forces in Europe cyber-only exercise Tacet Venari at Warrior Preparation Center on Einsiedlerhof Air Station, Germany, May 10, 2018 (U.S. Air Force/Blake Browning)

The Value of the Cyber Force

Senior political and military leaders recognize that our military must be able to compete below the level of armed conflict, and this idea is clearly stated in the National Security Strategy: "Our task is to ensure that American military superiority endures, and in combination with other elements of national power, is ready to protect Americans against sophisticated challenges to national security."[5] Nowhere is this requirement greater than in cyberspace, where peer competitors operate continuously against us in search of strategic advantage. To meet this intent, USCYBERCOM will:

- Operate forward and at scale where our adversaries are. This is the primary mission of cyber forces, which gives rise to U.S. Cyber Command's concept of defend forward. Its purpose is to limit the terrain over which the enemy can gain influence or control. We cannot afford to let adversaries breach our networks, systems, and data (intellectual property and personally identifiable information). If we are only defending in "blue space," we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.
- Assure the joint force can conduct operations securely and reliably. USCYBERCOM defends the DOD Information Network (DODIN), which is the command, control, communications, and data hub for the joint force. It facilitates nearly every phase of operations for the U.S. military. By defending the DODIN, USCYBERCOM has indirectly but strongly supported virtually every U.S. military operation launched since 2010. DOD relies on an increasingly secure and resilient information network to meet its full range of warfighting and enabling functions *because of past and ongoing USCYBERCOM operations.*

Enabling Capabilities for a Persistence Force

We are at a transformational moment for U.S. strategy and operations in cyberspace. Cyberspace represents a new strategic environment through which relative power can be challenged without resorting to armed conflict. Senior political and military leaders recognize that the initial approach that DOD took toward cyberspace aggression—focusing on resiliency and response actions—in effect committed the fundamental flaw in military operations of holding one's forces in reserve past the point of decision.

Fire controlman assigned to C4 cyber and intelligence department aboard USS *America* inspects surface-to-air intercept missile 162D on ship's missile deck, Pacific Ocean, August 31, 2017 (U.S. Navy/Alexander A. Ventura II)

Huntington identifies two other important factors that determine the success of a strategic concept: the resources, both human and material, required to implement it, and the organizational structure, which groups the resources allocated by society in a manner that implements the strategic concept. USCYBERCOM is maturing as a combatant command with the teams, infrastructure, tools, accesses, and authorities ready to execute missions. The command is also transitioning from force generation to a sustained readiness approach for persistent engagement with cyber adversaries and increased lethality in war. We continue to evolve the organization based on operational experience, task organizing, and employing small elements of teams in ways never anticipated when we stood them up.

One last factor that is crucial to success of a military element's strategic concept, which Huntington implied in his 1954 essay, is the ability of the commanders and the force itself to instill a sense of confidence among civilian leaders and the larger public that the element has devised an appropriate and viable strategic concept and has the skills to execute it on behalf of the Nation. The actions that follow from the strategic concept of persistent engagement should, over time, allow USCYBERCOM to install that sense of confidence. **JFQ**

Notes

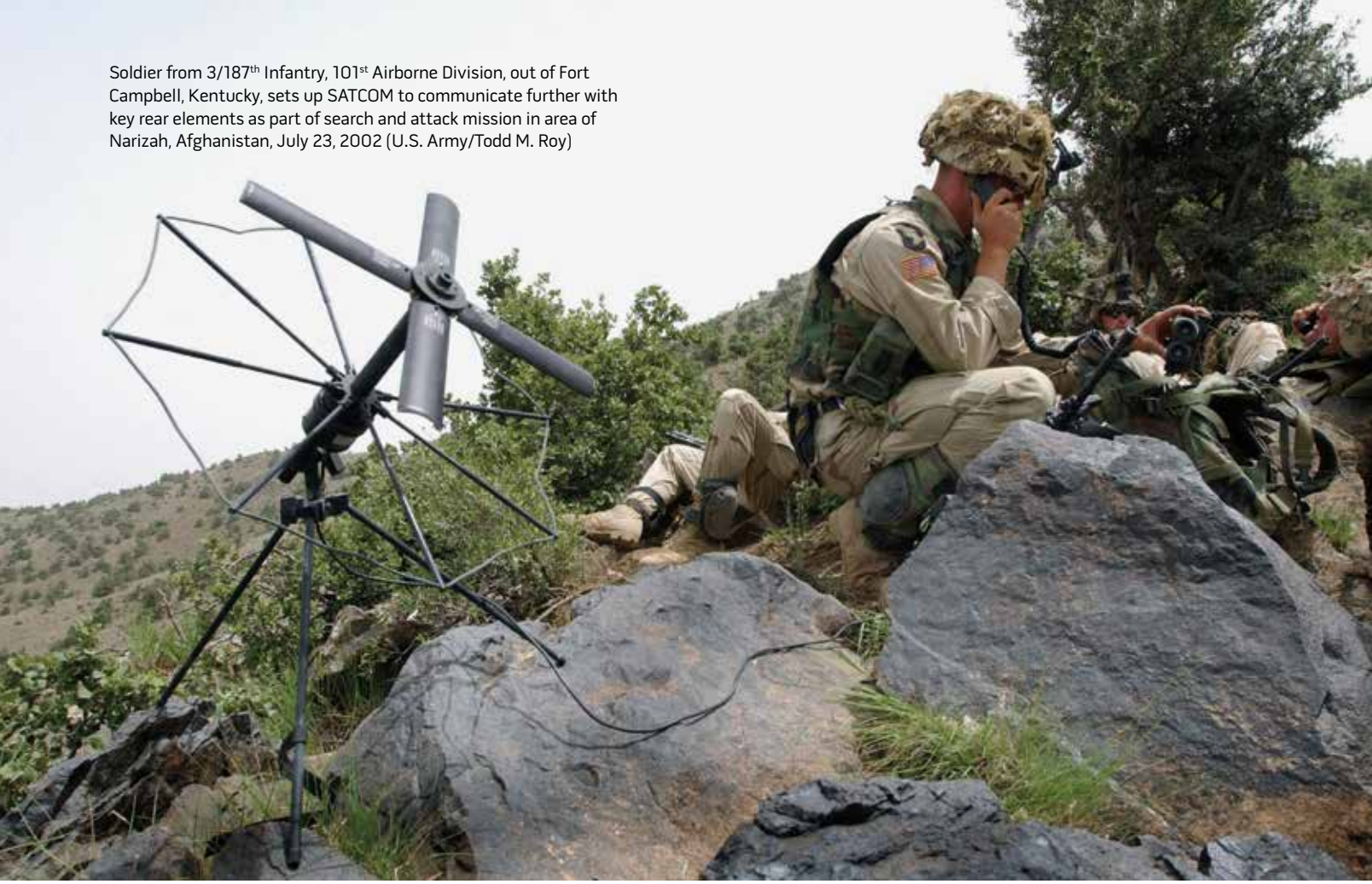
[1] Samuel P. Huntington, "National Policy and the Transoceanic Navy," U.S. Naval Institute *Proceedings* 80, no. 5 (May 1954).

[2] The Soviets had built a powerful navy by the 1980s, but they used it to control their local seas and protect their strategic missile submarines—not to contest control of the Atlantic or Pacific.

[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 170.

[4] *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: U.S. Cyber Command, March 2018).

[5] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 3.



Soldier from 3/187th Infantry, 101st Airborne Division, out of Fort Campbell, Kentucky, sets up SATCOM to communicate further with key rear elements as part of search and attack mission in area of Narizah, Afghanistan, July 23, 2002 (U.S. Army/Todd M. Roy)

Applying Irregular Warfare Principles to Cyber Warfare

By Frank C. Sanchez, Weilun Lin, and Kent Korunka

The cyberspace threat exists in a realm that does not conform to the physical limits of land, sea, air, and space. Unlike these traditional domains, cyberspace fosters an unpredictable threat that can adjust, morph, and reproduce without a national identity or face.[1] The challenge of the military is to posture its approach to cyberspace and cyberspace threats that are initiated by faceless, borderless, and sometimes nationless enemies. These enemies manifest in a domain neither confined nor governed by the traditional norms and rules of war, which the broader military has no experience undertaking. To ensure the United States maintains cyberspace dominance and can foresee, rapidly respond to, and counter cyberspace threats, the U.S. military's strategy and approach to cyberspace must adapt and incorporate unconventional approaches and hybrid warfare into its operational capability.

Despite its importance, the Nation's leaders, strategists, and military planners struggle to understand how cyberspace operations (CO) fit into national security as an instrument of national policy. A significant shortcoming is due to the leaders' lack of experience and basic understanding of what cyberspace is and what effects can be achieved in the cyber

Commander Frank C. Sanchez, USN, is an Action Officer on the Joint Staff J32, Intelligence, Surveillance, and Reconnaissance Operations. Major Weilun Lin, USAF, is Chief of the Central and South Asia Branch, Joint Cyberspace Center, U.S. Central Command. Lieutenant Colonel Kent Korunka, USA, is a Joint Intelligence Planner, Joint Planning Support Element, Joint Enabling Capabilities Command, U.S. Transportation Command.

Table. Conventional, Cyber, and Irregular Warfare

	Conventional	Cyber	Irregular
Purpose (why)	Gaining political, economic, ideological, social, and religious dominance via geolocation dominance for a period of time	Assisting in gaining political, economic, ideological, social, and religious dominance; gaining information for competitive advantage	Assisting in gaining political, economic, ideological, social, and religious dominance; gaining information for competitive advantage
Strategy (how)	Using overt operations and/or covert operations; showing might; little attribution issue	Using overt operations and/or covert operations; attribution issue	Using covert operations; attribution through intelligence
Involvement (who)	Some people such as military or paramilitary personnel	Everyone who has a device connected to affected networks	State and nonstate actors, adaptive adversaries such as terrorists, insurgents, and criminal networks
Targets (what)	Humans; mainly tangible objects; directly affecting human life	Mainly intangible items such as information or tangible items such as information systems; may indirectly affect human life in cyber physical cases	Humans; mainly tangible objects; directly affecting human life
Space (where)	Limited geolocaion	Anywhere with respect to geolocation if connected	Global
Duration (when)	A limited period of time	Ongoing, but one attack is usually within a short period of time	Very limited period of time
Preparation time (when)	Relatively long period of time	Relatively short period of time	Relatively short period of time
Cost (what)	Expensive	Relatively less expensive	Relatively less expensive
Characteristics (what)	Relatively more transparent	Relatively opaque and in stealth mode	Relatively opaque and in stealth mode
Attribution (what)	Relatively easy to find out	May be hard to find out	Relatively difficult to find out
Rules of engagement (what)	Relatively clear	Not clear	Not clear
Impression (what)	Always severe or brutal; obvious	Less severe if not life or death situation; sometimes not felt	Less severe if not life or death situation; sometimes not felt
Damage (what)	Severe with physical casualty	Severe with information loss	Sometimes severe
Direct impact upon (who)	Someone/some businesses	Everyone/every business connected to affected networks	Someone/some businesses
Impact based on (where)	Geolocation	Connection	Geolocation
Deterrence (what)	Obvious and forceful	Limited currently	Subtle
Dominance (what)	Could be achieved	Hard to achieve	Hard to achieve
Result/Gain (what)	Obvious	May not be very clear	May not be very clear
Winner (who)	Clear to identify	May be hard to decide	May be hard to decide
Time for recovering (when)	Relatively long	Relatively short	Relatively short

Source: Adapted from Jim Chen and Alan Dinerman, "On Cyber Dominance in Modern Warfare," in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, ed. Robert Koch and Gabi Rodosek (Reading, UK: Academic Conferences and Publishing International Limited, 2016), 54.

realm. Unlike the younger generation, who are considered digital natives, the majority of national and military leaders and military planners are considered digital immigrants. Popularized by Marc Prensky, the phrase *digital natives* refers to the generation who grew up using digital technology, and *digital immigrants* refer to the generation born before the advent of technology (circa the 1980s) but later adopted its use.[2] While digital immigrants lack cyber knowledge, many of them understand irregular warfare (IW) and the value and importance of special operations. The many similarities shared by IW and cyber warfare (CW) can establish a foundation to guide U.S. leaders in the execution of cyberspace operations to maintain cyber superiority.

Early cyber power theorists generally recognized three key terms: *cyberspace*, *cyber power*, and *cyber strategy*.[3] As the cyberspace domain matures, cyber theorists and thinkers still have not reached the appropriate definitions of these key terms. An understanding of irregular warfare fosters a rudimentary knowledge of cyber warfare. By highlighting how irregular warfare and cyber warfare are similar and providing the critical framework for using IW principles to approach, define, and integrate cyberspace operations across all domains and Services, U.S. leaders can begin to understand how cyber power can increase the effectiveness of the broader U.S. military cyber force.

Irregular Warfare and Cyber Warfare Interlinked

Special operations have a long, storied, and varied history within the U.S. military, including, for example, Roger's

Rangers, the assault of Pont-du-hoc, and Operation *Eagle Claw*. Colonel Joseph Celeski, USA (Ret.), noted that the Joint Special Operations University Special Operations Forces (SOF)-Power Workshop concluded that special operations is "a multi- and cross-domain force, capable of conducting or supporting conventional or unconventional operations on various levels leading to or supporting military and political outcomes."[4] Members of the workshop listed the following characteristics of the SOF operational environment:

- A complex operating environment marked by instability and ambiguity; acts of violence, influence, and leverage are conducted in a nonlinear and often indirect way and include low-level operations of subtlety and guile.[5]
- A high-risk, highly sensitive environment, in which there is high personal and political risk in conducting operations.[6]
- An irregular warfare environment characterized by intra-state and substate acts of political violence, plus insurgency, subversion, violent political action, and terrorism.[7]

Joint Publication 3-05, *Special Operations*, described the special operations environment as "hostile, denied, or politically and/or diplomatically sensitive . . . and . . . characterized by one or more of the following: time-sensitivity, clandestine or covert nature, low visibility, work with or through indigenous forces, greater requirements for regional orientation and cultural expertise, and a higher degree of risk."[8]

Cyberspace shares similarities with special operations due to its complexity and actors. The new global domain of cyberspace relies on the connected information technology infrastructure that includes all the automation and networked system components through which information or content flows or is stored.[9] Cyberspace operations are conducted in the physical network, logical network, and cyber-persona layers of the cyberspace domain.[10] The ease of entry into cyberspace allows individual actors, criminal organizations, and small groups to operate in the cyberspace environment on a similar level as nation-states and transnational organizations. The anonymity and lack of attribution afforded actors in the cyberspace domain resemble the covert or clandestine aspects of SOF.

The cyber domain threatens regional and national security in ways that are uncommon in the other traditional domains of land, sea, air, and space.[11] As a result, bad actors in cyberspace range from individual hackers and criminal enterprises to violent extremist organizations and nation-states. Bad actors steal information for personal or national gain for reasons that include profit, intelligence, denial of services, or to inflict damage on critical infrastructure. Within the traditional domains, these types of actions are relatively recognizable and easier to classify as acts of war, but in cyberspace the underlying intent and attribution of a cyber attack are difficult to discern.

Past thinkers and strategists have identified other similarities between special operations and cyber operations. Eric Trias and Bryan Bell wrote, "The inherently clandestine nature of special operations parallels the ease of conducting stealthy cyber operations."[12] Patrick Duggan proposed that "cyber-warfare is, at its core, human-warfare" and "requires SOF's unique human expertise, unconventional mindsets, and discreet asymmetric options."[13] Most notably, Jim Chen and Alan Dinerman presented a framework to compare and contrast the similarities between conventional warfare and cyber warfare. Using factors borrowed from other authors, Chen and Dinerman created a matrix to facilitate the discussion of the cyber warfare capabilities compared to conventional warfare.[14] An adaptation of their findings is reflected in the table, which includes IW for comparison and contrast, in order to highlight the similarities between CW and IW. While not entirely inclusive of all aspects and characteristics of each warfare, the table illustrates the strong parallels between cyber warfare and irregular warfare.

Despite the many similarities highlighted in the table, it is important to recognize the differences between CW and IW. A key difference, low personal risk, is the greatest strength of cyber warfare. Cyber attacks can be conducted from almost anywhere while still within the confines and relative safety of a nation-state's geographical boundaries. The low personal risk of CW lies in stark contrast to the high personal risk assumed by SOF personnel conducting missions in highly contested environments or deep behind enemy lines. The low personal risk of CW is further supported by the ease of entry into cyberspace and the lack of attribution so long as appropriate steps are taken to conceal identities.

Many core activities of special operations seamlessly fold into the context of cyberspace missions. Offensive cyberspace operations are similar to the intent of special operation's direct action, countering weapons of mass destruction, military information support operations, and special reconnaissance missions. Likewise, the intent of special operation's foreign internal defense and security force assistance missions compare to defensive cyberspace operations.[15] While the cumbersome process to identify and attribute the actor, target, and effect of cyber attacks and information to a nation or group is significant, the necessity for overt nation-state versus nation-state engagement is not as profound. Operations in cyberspace should espouse undetected intrusion where the potential for monitoring, destabilizing, and manipulating provides greater long-term gain than immediate destruction or devastation.

The U.S. approach to CW would likely best benefit from mirroring special operations, IW, and the SOF community, which rely on highly specialized and unique tactics, techniques, procedures, and equipment. At its core, irregular warfare is about the "highly adaptive actors." Rain Ottis and Peeter Lorents wrote, "Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems."[16] They stress the fact that "cyberspace is an artificial space, created by humans for human purposes," which requires the need to understand and influence peoples' thoughts and actions.[17]

Soldier assigned to 2nd Armored Brigade Combat Team, 1st Cavalry Division, conducts dismounted electronic warfare training at Fort Hood, Texas, August 29, 2018 (U.S. Army/Carson Petry)

Applying Other IW Principles to Cyber

Because of the similarities, the next logical step is to cross over special operations and IW terminologies to build on the foundation of thought and theory regarding cyber warfare. In the paper "Adapt Special Operations Principles to Cyber," Nicholas Co recommended the application of SOF Truths, created by Colonel Sid Shachnow, USA, in the mid-1980s, as guiding principles that will support success in future cyberspace operations.[18] The special operations construct is built on individuals, small units, and advanced technology. The first SOF Truth recognizes that its personnel rather than the equipment are what gives special operations its decisive edge. It is highly trained people applying highly specialized skills with flexibility, creativity, and innovation along with unique capabilities that achieve national objectives across a wide array of military options.[19] Along those lines, the article introduces several other concepts and terminologies adapted from the SOF community.

First, the concept of relative superiority used in irregular warfare should be applied to cyberspace operations. In his book *Spec Ops*, Admiral William McRaven defined the term *relative superiority* as "a condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well-defended enemy."[20] As noted earlier, ease of entry into the cyberspace domain requires low personal risk as it enables a force as small as an individual hacker to overwhelm or operate against a well-defended adversary at a potential point in time. A common misconception exists that global cyber dominance or supremacy is possible and easily maintained. William Bryant quoted the argument from noted cyber expert Martin Libicki that "cyber supremacy is meaningless and, as such, is not a proper goal for operational cyber warriors."[21] The Joint Operating Environment 2035 envisions a future security environment full of vulnerable points through which weapons systems can be directly engaged and military operations have global reach to individual work stations, servers, routers, or controller chipsets.[22] The broad and dynamic nature of cyberspace, consisting of countless devices, makes it impossible to maintain total cyber superiority. This is a persistent risk where at any point in time, one may lose relative superiority. The recent release of U.S. Cyber Command's "Command Vision" highlighted this by stating, "New vulnerabilities and opportunities continually arise as new terrain emerges. No target remains static; no offensive or defensive capability remains indefinitely effective; and no advantage is permanent. The well-defended cyber terrain is attainable but continually at risk."[23] In Air Force Doctrine Document 3-12, *Cyber Operations*, the Air Force defines *cyberspace superiority* as "the operational advantage in, through, and

from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference."[24] This definition closely aligns with Admiral McRaven's comment that relative superiority is achieved at the *pivotal moment in an engagement*.[25]

Second, the term *superiority* alludes to the ability to project a type of power on an adversary—*cyber power*. But the Department of Defense (DOD) does not have a definition of cyber power. The closest DOD definition is the Air Force's definition of *cyberspace force application* as "combat operations in, through, and from cyberspace to achieve military objectives and influence the course and outcome of conflict by taking decisive actions against approved targets."[26] To define *cyber power*, John Sheldon uses the following: "the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment."[27] By adapting SOF concepts and terminology to these previous definitions, this article proposes the following definition as a springboard for additional thought and discussion on cyber power. At the strategic level, cyber power is the combined strength of a nation's cyberspace capabilities to conduct and influence activities in, through, and from cyberspace to achieve national security objectives in peacetime and across the full spectrum of conflict. At the operational and tactical level, it is also the control and relative superiority gained by application of cyberspace operations over an adversary that uses technology as a means to contest integrity, confidentiality, security, and accessibility of information.

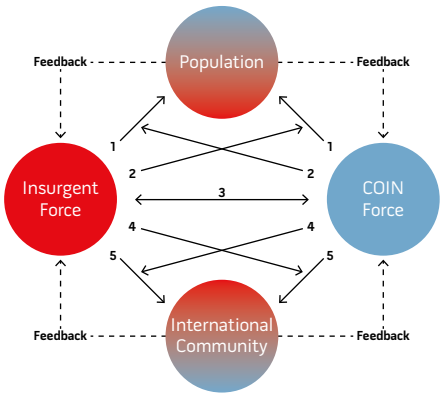
Irregular Framework for Cyberspace Strategy

Today there is a multitude of perspectives and frameworks for cyber strategy. The operational environment influences strategy because strategy must anticipate the changes in the operational environment.[28] DOD utilizes central aspects of the cyber threat such as threat actors, insider threats, supply chain vulnerabilities, and threats to DOD operational ability for developing its strategy for cyberspace operations.[29] Some strategies are only oriented toward cyber defense or cyber security while other strategies are offensive in nature. Principles and theories from Gordon McCormick's "Counterinsurgency Diamond Model" can be applied as a framework for developing a holistic approach or strategy for cyberspace operations. For this article, a brief explanation of McCormick's model in its context and framework would allow application of its overall premise to cyberspace. As shown in figure 1, Greg Wilson briefly describes the model's utilization and interactions:

The Diamond Model establishes a comprehensive framework that considers the interactions between the state or host-nation government, the insurgents or terrorists, the local populace, and international actors or sponsors. The state or the "host nation" government's goal is to destroy the insurgents or limit their growth and influence to a manageable level. The insurgent or terrorist goal is to grow large enough to destroy the state's control mechanisms and replace the existing government or force some form of political concession from the government that achieves their desired goals. To develop an effective strategy, the state must first understand its advantages and disadvantages relative to the insurgents. The state, which normally has an established security apparatus consisting of armed forces and police, has a force advantage over the insurgents but suffers from an information disadvantage. This information disadvantage stems from the fact that the insurgents or terrorists are difficult to detect and target because they are dispersed and embedded in the local populace.[30]

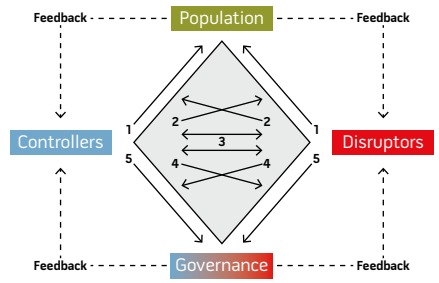
The Cyberspace Diamond Model, shown in figure 2, is based on McCormick's Counterinsurgency Diamond Model and promotes information legitimacy in cyberspace through good governance, improved security, and transparency (as related to attribution). Information legitimacy is at the heart of the cyberspace conflict, as it is received and perceived by all actors within the

Figure 1. McCormick's Counterinsurgency Model



Source: Gordon H. McCormick, "Seminar in Guerrilla Warfare," Naval Postgraduate School, Monterey, CA, 2003.

Figure 2. Cyberspace Diamond Model



Source: Adapted from McCormick's Mystic Diamond Model (McCormick, "Seminar in Guerrilla Warfare," Naval Postgraduate School, Monterey, CA, 2003).

operational environment. National leaders and military professionals should utilize this Cyberspace Diamond Model to frame their strategic approach to cyber warfare. This framework, however, can also be implemented at the operational and tactical levels to aid military leaders and planners in translating strategic direction into operational plans.

The Controllers. Controllers are the current influential or administrative force of a section of cyberspace, or information communication technology (ICT). Examples of controllers can range from network administrators to national governments. Generally, there is a single force that is the lead, but the private sector, organizations, or countries can provide additional capabilities to augment the controllers. The controllers

Air Force Institute of Technology students listen as professor (right) explains hacking technique during class at Wright-Patterson Air Force Base, Ohio, February 20, 2018 (U.S. Air Force/Al Bright)

must integrate all instruments of national power—civil, military, diplomatic, information, economic, technology, and financial. These forces include but are not limited to policymakers, military, law enforcement, intelligence, infrastructure providers, and cyber security personnel. Controllers are defined by the disruptor's perceptions, but external forces can be perceived by the disruptors as influencing the situation, and, consequently, those forces become part of the controllers. The same is true of the controllers defining the disruptors; however, the controllers typically have a greater burden of proof as dictated by global perceptions. Attribution is the greatest hurdle for the controllers to overcome.

The Disruptors. Disruptors are the humans, machines, governments, and criminals conducting or supporting operations to interrupt or disturb the availability, security, confidentiality, or integrity of information in cyberspace. Disruptors are also anyone or anything that is either actively or passively *supporting* disruptors. There is not always a clear distinction between voluntary disruptors and those coerced into supporting disruptors. For example, computers in a botnet that are maliciously controlled without the owners' consent can be considered coerced (involuntary) disruptors. Disruptors conduct exploitation of the population's trust to gain support or control.

The Population. The population consists of the user in cyberspace or the ICT—humans or machines. While support may be coerced out of the population, the population is not considered disruptors until it provides additional support beyond what is required. The population serves as the source of power in both diamond models. However, in cyberspace, the operational environment extends past geographic borders where the population can be global, regional, or an individual system user.

Governance. Although cyberspace lacks the normal rule of law and traditional notion of governance, this article incorporates the term of governance based on the United Nations Educational, Scientific, and Cultural Organization's (UNESCO's) definition. UNESCO defines it as "*structures and processes* that are designed to ensure accountability, transparency, responsiveness, rule of law, stability, equity and *inclusiveness, empowerment, and broad-based participation*."[31] UNESCO also refers to it as "the norms, values and rules of the game" and "about the culture and institutional environment in which citizens and stakeholders interact among themselves and participate in public affairs."[32] As one of the actors in the Cyberspace Diamond Model, governance consists of external nation-states, international organizations, and other groups that do not function in a direct or indirect support role for the controllers and disruptors. Members of the governance, similar to the population, remain neutral until they provide support to a side; once support is provided (or perceived to be provided), they become controllers or disruptors.

The legitimacy of an organization or entity may be placed upon or perceived by the actors within cyberspace. Examples of governance, perceived or placed upon by the population, are the National Institute of Standards and Technology, WikiLeaks, or Hypertext Protocol.

Framing Cyber Strategy and Feedback

Controllers and disruptors must conduct every operation in consideration of how it will affect the perceived legitimacy of the information that is received by the population and governance. As shown and numbered on the Cyberspace Diamond Model, the controllers and disruptors will use all five of the following strategies throughout the cyberspace conflict; however, the source of power, as noted, is primarily the population. Cyberspace enables controllers to focus on direct action against the disruptors by utilizing cyber attacks. It is important to note, however, that controllers must recognize the significance of maintaining the security, accessibility, integrity, and confidentiality of the population's information. As a result, emphasis is placed on strategies 1 and 5 as both forces must execute elements of each strategy.

Strategy 1: Population Support. In figure 2, the intent of strategy 1 is to gain the support of the source of power-—the population—since both controllers and disruptors rely on popular support for success. Although controllers are generally strong in resources, personnel, and cyberspace capabilities, they normally lack specific intelligence on the disruptors. Therefore, controllers need popular support to gain the required intelligence to identify the disruptors. This is similar to the IW interaction between the counterinsurgency or insurgency forces and the population. Controllers promote information legitimacy through good governance, improved security, and socioeconomic conditions in cyberspace. The goal of controllers is to maintain its control of the operational environment, the legitimacy of their information, and the trust of the population. Securing and maintaining the support of the population will cost the controllers a substantial amount of resources, time, capabilities, and manpower.

Building 92 at Microsoft Corporation headquarters in Redmond, Washington, May 30, 2016 (Courtesy Coolcaesar)

Strategy 2: Information Disruption. As depicted in figure 2, the intent of strategy 2 is to prevent or interrupt the opponent's control of the population. The objective of the controllers is to create a divide between the disruptors and population by delegitimizing the disruptors' information and denying them access and freedom of movement to, from, and through the population and other resources in the operational environment. Disruptors must attempt to delegitimize information transmitted through cyberspace and ICTs or break or disrupt the controllers influence over the population and resources that disruptors depend on. Strategy 2 favors the disruptors due to ease of attack on the information legitimacy of the controllers as compared to the challenging task of the controllers to attack the information legitimacy of the disruptors. Transparency and accountability are key to the success of the controllers. Similar to IW, it is easier for insurgents to attack the legitimacy and control of governments.

Strategy 3: Direct Action. Strategy 3 is directed at striking the opponent to disrupt his operations and deny his will and ability to continue the conflict. The controllers' broad, sweeping, and obvious signature enables the disruptors to identify the activities and locations of controllers, which therefore increases the level of personal risk to the controllers. This knowledge enables disruptors to conduct attacks at the time and location of their choosing, thereby potentially reducing collateral damage or attribution. Because the operational environment can be expansive, controllers must first gain intelligence before it can conduct effective operations against disruptors. Indiscriminate assaults can delegitimize the governance of the ICTs and thereby lose the support of the population. An example of indiscriminate assaults is a government's mass censorship of information in cyberspace.

Strategy 4: Disrupt Interaction. Both forces require perceived legitimacy to obtain support and access to governance in strategy 4. The recent Shadow Brokers (disruptors) leak of National Security Agency secrets and capabilities serves to disrupt information legitimacy between the U.S. Government (controllers) and Microsoft (governance). Microsoft has perceived governance because it is responsible for providing vulnerability and security patching and fixes for its products. Using the Cyberspace Diamond Model, the U.S. Government (controllers) needs to attack

the information legitimacy of the Shadow Brokers (disruptors), while boosting their relationship, interaction, and trust with Microsoft (governance).

Strategy 5: Governance Relationship. Strategy 5 outlines that at the nation-state level, the legitimacy of governance and strong international backing can provide perceived information legitimacy. At that level, this is stressed through the whole-of-nation approach and strong international cooperation. The global interlink of cyberspace and ICTs are only as strong as its weakest and most vulnerable link.

Feedback. Feedback is critical in understanding the effects of controllers' and disruptors' actions on popular and international perceptions. The feedback connections allow both forces to assess the success or failure of their cyberspace operations toward information legitimacy. Both sides must establish and maintain feedback mechanisms to assess their operations.

Recommendations and Conclusion

Despite the establishment of U.S. Cyber Command to engage and operate in the youngest warfighting domain, a precise understanding of cyberspace and operations within still remains elusive. The lack of understanding can lead to a miscalculation in the use of cyber forces and capabilities in execution or support of national objectives. Cyber theorists and national leaders must recognize how IW concepts and theories can be applied to cyberspace operations. The basis of their similarities lies in their complexity, highly adaptive actors, and operational environment, which is not limited by traditional geographic boundaries. By comprehending the similarities between CO and IW characteristics, principles, and theories, leaders at the strategic, operational, and tactical levels can frame their thought process and formulate coherent plans.

Through the IW lens, our leaders begin to understand that cyber warfare can be conducted in combination with or independent of conventional military operations. Cyberspace operations against state and nonstate actors should be conducted in protracted regional and global campaigns, often beneath the threshold of overt war.[33] Furthermore, our cyber strategies require a whole-of-nation and/or a whole-of-international-coalition approach to obtain relative superiority in the dynamic cyberspace operational environment. By utilizing the Cyberspace Diamond Model to frame cyberspace strategy at the strategic, operational, and tactical levels, military leaders and planners can translate strategic direction into operational plans for the cyber domain. **JFQ**

Notes

[1] Patrick Lichty, *Variant Analyses Interrogations of New Media Art and Culture* (Amsterdam: Institute of Network Cultures, 2013), 54.

[2] Marc Prensky, "Digital Natives, Digital Immigrants," *On the Horizon* 9, no. 5 (October 2001).

[3] Sean Charles Gaines Kern, "Expanding Combat Power Through Military Cyber Power Theory," *Joint Force Quarterly* 79 (4th Quarter 2015).

[4] Joseph Celeski, *A Way Forward for Special Operations Theory and Strategic Art*, Joint Special Operations University SOF-Power Workshop, August 2011, MacDill Air Force Base, 15.

[5] Ibid., 15–16.

[6] Ibid.

[7] Ibid., 16.

[8] Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: The Joint Staff Staff, 2014), ix.

[9] JP 3-12 (R), *Cyberspace Operations* (Washington, DC: The Joint Staff Staff, 2013), I-2.

[10] Ibid.

[11] Ibid., I-7.

[12] Eric D. Trias and Bryan M. Bell, "Cyber This, Cyber That . . . So What?" *Air & Space Power Journal* 24, no. 1 (Spring 2010), 95.

[13] Patrick Duggan, "Why Special Operations Forces in U.S. Cyber-Warfare?" *Cyber Defense Review*, January 8, 2016.

[14] Jim Chen and Alan Dinerman, "On Cyber Dominance in Modern Warfare," in *Proceedings of the 15th European Conference on Cyber Warfare and Security*, ed. Robert Koch and Gabi Rodosek (Reading, UK: Academic Conferences and Publishing International Limited, 2016), 54.

[15] JP 3-12 (R), *Cyberspace Operations*, vii.

[16] Rain Ottis and Peeter Lorents, "Cyberspace: Definition and Implications," Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 268.

[17] Ibid.

[18] Nicholas Co, "Adapt Special Operations Principles to Cyber," U.S. Naval Institute *Proceedings* 143, no. 6 (June 2017), 58–59.

[19] JP 3-05, *Special Operations*, I-2.

[20] William H. McRaven, *Spec Ops, Case Studies in Special Operations Warfare: Theory and Practice* (New York: Random House, 1995), 4.

[21] William D. Bryant, "Cyberspace Superiority: A Conceptual Model," *Air & Space Power Journal* 27, no. 6 (November–December 2013), 25, available at <www.airuniversity.af.mil/Portals/10/ASPJ/jthenals/Volume-27_Issue-6/F-Bryant.pdf>.

[22] *Joint Operating Environment (JOE 2035): The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, July 14, 2016), 36.

[23] *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD: U.S. Cyber Command, 2018), 4.

[24] Air Force Doctrine Document (AFDD) 3-12, *Cyber Operations* (Washington, DC: Headquarters Department of the Air Force, July 15, 2010, incorporating Change 1, November 30, 2011), 50.

[25] McRaven, *Spec Ops, Case Studies in Special Operations Warfare*, 4. Emphases by authors.

[26] AFDD 3-12, 50.

[27] John B. Sheldon, "Deciphering Cyberpower: Strategic Purposes in Peace and War," *Strategic Studies Quarterly* (Summer 2011), 95–112.

[28] JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 2017), III-2.

[29] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 3.

[30] Gregory Wilson, "The Mystic Diamond: Applying the Diamond Model of Counterinsurgency in the Philippines," in *Gangs and Guerrillas: Ideas from Counterinsurgency and Counterterrorism*, ed. Michael Freeman and Hy Rothstein (Monterey, CA: Naval Postgraduate School, April 2014), 15. To gain a better understanding of the Diamond Model, see Gregory Wilson, "Anatomy of a Successful COIN Operation: OEF-Philippines and the Indirect Approach," *Military Review*, November–December 2006.

[31] United Nations Educational, Scientific, and Cultural Organization, "Concept of Governance," International Bureau of Education, available at <www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance>. Emphases by authors.

[32] Ibid.

[33] *Achieve and Maintain Cyberspace Superiority*, 2, 7.

Airmen and Soldiers from Kadena Air Base perform high-altitude, low-opening jump off MC-130J Commando II above Okinawa, April 24, 2017 (U.S. Air Force/John Linzmeier)

Toward a More Lethal, Flexible, and Resilient Joint Force

Rediscovering the Purpose of JPME II

By Charles Davis and Frederick R. Kienle

The defense and military strategies of Secretary of Defense James Mattis and Chairman of the Joint Chiefs of Staff Joseph Dunford thoughtfully focus the joint force in order to meet transregional, multidimensional, and multifunctional threats to U.S. national security. In addition to advanced capabilities and integrating concepts, another critical enabler for a more lethal, flexible, and resilient joint force is greater *jointness*. Jointness, which embodies trust, cooperation, and interdependency, continues to develop across the Armed Forces and has proved to be integral to success on modern battlefields. Today's complex security environment demands truly joint warfighters who are capable, comfortable, and confident when operating across functions, domains, and cultures. A process for acquiring this critical enabler already exists but is largely disregarded. The Department of Defense (DOD) must rediscover the process if it is to succeed in building the levels of trust and interoperability called for in the 2018 National Defense Strategy.[1]

The panel on military education led by Congressman Ike Skelton in the late 1980s restructured joint education to overcome Service parochialism that beset past military operations. Reforms under

Dr. Charles Davis is an Associate Professor in the Joint Forces Staff College at the National Defense University. Colonel Frederick R. Kienle, USA (Ret.), Ph.D., is a Professor at the Joint Forces Staff College and was the first Director of the Joint Advanced Warfighting School. He has served on 26 Process for the Accreditation of Joint Education teams.

the Goldwater-Nichols Department of Defense Reorganization Act of 1986 sought to advance jointness within the U.S. military, and, since then, many have trumpeted its success in improving the efficacy of the joint force. Of the three phases of joint professional military education (JPME) created by the Skelton Panel, the second phase, JPME II, is unique with its requirement to substantively acculturate military officers to the different Service cultures. The panel decided that among the four directed outcomes of JPME II the most important is the development of "joint attitudes and perspectives."[2] The panel keenly understood that officers possessing these qualities are imperative to increasing the effectiveness of joint operations. Sustaining and advancing jointness is an ongoing, transformative effort—it is a journey and not an endstate—and the panel's reforms to joint education were the centerpiece of the legislation. The path to greater jointness was well designed within the context of JPME II, and the role of joint acculturation in the process stood front and center. Not only was JPME II expected to prepare officers for their first joint assignment, but it was also designed to inculcate the trust and common understanding essential to jointness.

Three decades after the reforms, however, the understanding and vision established by the panel have faded. The ability to foster greater jointness through JPME II is endangered by those who misunderstand or underappreciate both its principal outcome and preparatory nature. The Chairman's accreditation of programs for the delivery of JPME II has not always considered the true ability of these programs to achieve the mandated outcome: the development of joint attitudes and perspectives through the joint acculturation of students. For reasons of mission, goals, and structure, this outcome is unlikely to be equal across programs, much less assured. And, with historical consistency, a large proportion of officers do not attend JPME II before their initial joint assignments. The failure to prepare officers for joint assignments unnecessarily burdens joint commands with members who rigidly embrace and advocate Service-centric approaches to joint problems because they were not educated otherwise. Avoiding or forfeiting the opportunity for acculturation and inculcation of jointness before embarking on a joint assignment places officers, their supervisors, and their commands in a needlessly disadvantaged position.

In effect, DOD fails to establish the full range, maturity, and sustainability of jointness it otherwise should. Jointness derives from the integration of different Service cultures and competencies, and it requires teamwork, unfettered by parochialism, among all Services and military departments.[3] Jointness exists nowhere if not in the *mental* realm, which means that jointness is perishable and must be cultivated—continuously. JPME II is the keystone educational experience for cultivating broader and deeper joint attitudes and perspectives within the force. For this reason, DOD must reflect on and recalibrate its approach to joint education and, in particular, JPME II, if it is to enable the joint force to prevail over the priority challenges it faces.

The Importance of Joint Attitudes and Perspectives

The future security environment requires targeted investment in new capabilities and growth in the number of platforms. But genuinely increasing the lethality, flexibility, and resiliency of the joint force depends on investment in people as well. DOD must broaden and deepen jointness in the force beyond what has already been achieved—to develop *more* officers who are even *more joint-minded* than their predecessors. Such officers value the contributions of the other Services more and trust their members more willingly when working together as a joint team. Only in this way can the joint force reach the level of interdependence required to most effectively employ new capabilities and platforms because jointness remains contingent on how Servicemembers think and feel—it is not merely a collection of capabilities and platforms.

Jointness is nothing if it is not valued by officers belonging to different Service cultures who must be willing to trust each other while collaborating to accomplish joint military objectives. These characteristics are not easily fostered by the powerful Services as they train, educate, and culturally indoctrinate their members. Most often, Service parochialism and bias are the usual outputs, and this means joint attitudes and perspectives must be cultivated externally. The JPME system develops military officers along three axes: character—ethical and moral leadership; joint acculturation—learning from one's peers; and intellectual development—critical thinking and mental agility.[4] Of the axes, joint acculturation is the most critical when the goal is to produce effective joint officers. With the creation of JPME II, the aim of the Skelton Panel was to instill joint attitudes and perspectives in officers headed for joint duty, and to achieve "nothing short of a change in the culture of the officer corps" through a socialization process requiring both time and emphasis.[5] This socialization process, or joint acculturation, is what sets JPME II apart from the other phases of joint education—no other phase requires instilling joint attitudes and perspectives in students as the principal outcome.

The Skelton Panel described the creation of joint attitudes and perspectives only in general terms, and existing law and military policy fail to describe or define the process of joint acculturation that makes JPME II unique. But the panel intended for JPME II to be in-residence only, multi-Service in composition, and conducted on neutral, non-Service-centric ground in order to achieve joint acculturation.[6] The panel's conditions are crucial because optimal acculturation requires structured, meaningful, and purposeful contact between members belonging to different cultures. Knowledge of the preconditions for achieving acculturation stipulate the educational requirements. In the context of PME, those requirements mean JPME II students must work collaboratively toward a common goal—a condition where they must cooperate for everyone to succeed. It also means that such activity must occur within a culturally neutral venue where student seminars are balanced in Service representation and with minimal

disparity in rank.[7] Qualitative joint acculturation outcomes for officers of different Services are also governed by a calibrated balance between the intensity of collaboration, the duration of their contact, and the quality of their experience. In this way, Service-centric views and biases are quickly challenged and substantially reduced. As a result, officers can more capably consider joint approaches to military problems and more willingly trust those from different Services during planning and execution.

Better and timelier preparation of joint officers increases the effectiveness and warfighting lethality of the joint force. The Skelton Panel understood this as well and carefully highlighted the preparatory nature of JPME II, implying that such education and socialization would achieve the greatest utility and benefit when received by officers en route to their initial joint assignment.[8] In the panel's model, officers liberated from a Service-centric mindset could, as a member of a joint staff, more effectively and productively develop solutions to complex military problems. Joint-mindedness on the part of officers has inarguably become even more important.

As the U.S. military strives to more broadly adopt the philosophy of mission command—operating through empowerment and understanding in a world of multidimensional threats—it must recognize that trust is one of the most important elements.[9] Affect-based trust is the outgrowth of joint acculturation, and officers must internalize this trust *before* forces and functions are brought together in crisis. Joint education and development must necessarily include preparation and joint acculturation to build joint teams, but DOD has lost sight of that end.

Has the Purpose of JPME II Been Forgotten?

While the earlier reforms to joint education have undoubtedly contributed to an unprecedented level of jointness in the force over the last few decades, DOD is moving away from the two most important aspects of JPME II. In practice and legislation, this phase of joint education, among others, has seen significant modification in the last two decades, and this has given rise to concerns regarding its purpose, timing, and, by extension, its effectiveness.[10]

This is because efforts by DOD to expand the number of joint educated officers has led to a proliferation of JPME II–accredited institutions, where most have joint acculturation as a secondary or tertiary objective at best. The most important purpose of this phase of joint education is to instill joint attitudes and perspectives in officers through joint acculturation, but JPME II has now taken on many different forms and meanings. The cumulative result of those past and present efforts to expand joint education is that there are now no less than 13 different JPME II–accredited programs within DOD, and most of the programs exist for purposes and missions far apart from instilling joint attitudes and perspectives. These programs must somehow balance their traditional Service and specialty emphasis with the myriad needs of joint force curricula, while simultaneously trying to instill joint attitudes and perspectives.

Rather than creating a deeper pool of truly joint-minded warriors, efforts to expand JPME II appear to have been driven by pressures either to generate a larger pool of joint-qualified officers from which the Services could promote to flag or general rank or to protect particular programs from the chopping block. The Services wanted JPME II accreditation in order to afford their war college students the opportunity to obtain JPME II credit without necessarily attending a separate course designed around acculturation and specific preparation for a joint assignment. In these decisions, jointness and joint acculturation have taken a back seat.

Each program uses a different approach and intensity to foster joint acculturation. The problem is that there is little demonstration of whether and to what degree these programs are achieving the principle JPME II outcome, much less how their outcomes compare to a program specifically missioned and structured for the purpose of joint acculturation, such as the Joint and Combined Warfighting School in Norfolk, Virginia. The lack of emphasis on joint acculturation was evident when DOD accredited the Service war colleges based on the provision that they could maintain a modicum of representation from the other Services in their student body and faculty.[11] Service culture predominance is unavoidable in the Service colleges. The Skelton Panel observed that these institutions would always have a continuing tension between fostering joint acculturation and maintaining their distinct Service cultures.[12] For this reason, the panel insisted that JPME II be taught from a joint perspective and at a culturally neutral location.[13] The panel's requirements for genuine acculturation have generally been abandoned over time.

The Process for Accreditation of Joint Education (PAJE) is the means for certifying that all JPME programs fulfill the respective learning areas and objectives prescribed in DOD policy and in statute. Recently, several PAJE accreditation team visits found insufficient emphasis and focus on jointness and, in some cases, a concerning lack of commitment to teaching the fundamentals of joint warfighting. While helping to uphold the legal and intended standards of JPME II, the PAJE identified several programs that lack the requisite emphasis and effort to truly develop joint awareness, perspectives, and attitudes. A large part of this problem lies with the Chairman's Officer Professional Military Education Policy (OPMEP), which details the learning areas and objectives for all JPME programs. Not surprisingly, prescribed learning areas and objectives vary substantially across JPME II–accredited programs, of which only two are categorically charged to "cement" joint attitudes and perspectives.[14] The lack of focus on acculturation and on the deliberate development of joint perspectives and attitudes, as evidenced in multiple accreditation reviews, illuminates a problem that evolved over time.

The OPMEP also describes seven common educational standards for JPME, the first of which is to "develop joint awareness, perspective and attitudes."[15] This standard does little to

Marines with Black Sea Rotational Force 18.1 advance to their objective during patrolling exercise at Army base Nova Selo Forward Operating Site, Bulgaria, May 10, 2018 (U.S. Marine Corps/Angel D. Travis)

encourage or achieve acculturation, however, because the measures are largely confined to the degree of Service representation among the students (and faculty) in the JPME institutions, along with a broad review of curriculum content.[16] In the case of Service war college JPME II programs, the statute allows 60 percent of the students to be from the host Service in a single Service institution focused on the outcomes, competencies, and cultural goals of that Service. The common educational standard does not adequately stress the achievement of true joint acculturation, which is characterized by discernable changes in attitudes and perspectives through a truly joint environment where Service representation among faculty and students is balanced. Too often, at some Service JPME II institutions, the PAJE reveals that acculturation was an afterthought.[17]

The evidence to demonstrate attainment of acculturation may be difficult to find, but the efforts to achieve true joint acculturation within a variety of approaches are generally unmistakable. The large variance in OPMEP-prescribed learning areas and objectives, compositional imbalances in student and faculty populations, and Service-centricity in curriculum and organizational goals virtually assure disparity in joint acculturation outcomes. Yet the absence of common JPME II requirements and a validated measure of the acculturation outcomes of the various programs restrict the PAJE to only a vague assessment of what a particular program might be doing to foster joint acculturation, and not whether it is in fact achieving success.

No Longer "Right Officer, Right Time"

In addition to overlooking its principle focus of joint acculturation, the value of JPME II to the individual officer is diminished when not received in advance of his or her initial joint assignment. The Skelton Panel discussed the importance of timely joint education when conceiving of its educational reforms; panel members focused both on which Servicemembers and when Servicemembers receive joint education. Ideally, an officer headed for initial joint duty should receive Phase II while en route to that assignment—a circumstance often referred to as "right officer, right time." Much of the defense establishment is, however, dismissive of the preparatory nature of JPME II and the joint acculturation it is intended to provide. Such derision is in part attributable to DOD-sponsored legislative changes that inadvertently weakened the connection between JPME II and joint duty assignments.

For instance, the 2007 National Defense Authorization Act approved a new Joint Qualified Officer (JQO) system under which officers must complete JPME I and II prior to becoming JQOs, but unlike the previous system it no longer requires them to do so prior to serving in a joint duty assignment.[18] The decoupling of JPME II and initial joint duty requirements eased pressures on Service personnel systems and provided convenient options to personnel managers but shortchanged student academic

and cultural experiences. Worse, it bolstered beliefs that JPME II is merely a "check in the box" requirement rather than an essential joint educational, socialization, and preparatory experience. Such institutional devaluing occurred because Service personnel managers were allowed to view JPME II only as a qualifier for promotion to general or flag officer. Not surprisingly, within 3 years of this change two prominent studies indicated that many officers serve in joint assignments without adequate educational preparation. One report, sponsored by DOD, observed that it is "the exception instead of the rule that a staff officer gets to attend JPME prior to a combatant command assignment."[19] The second report, a congressional study of PME, also found that many officers are sent to joint duty assignments without JPME II and that the practice disregards the fundamental purpose of the education.[20] The failure to prepare officers for joint duty means that officers are relegated to learning joint attitudes and perspectives on the job. Such an approach guarantees inconsistency in officer learning and risks reinforcement of, rather than correction to, Service-centric views and biases. Being the "right officer" means receiving the right education at the "right time," which is before an officer's initial joint assignment. DOD can and must do better.

The proportion of officers receiving JPME II ahead of their initial joint assignment has never been ideal, but disordering the two has become an accepted and endemic practice. This is despite awareness among many within DOD that the learning curve for officers arriving at a combatant command is particularly long and steep—disproportionately so compared to typical Service assignments.[21] With recent DOD-sponsored legislation reducing the requisite time in a joint assignment to achieve joint duty credit, the imperative for preparatory education becomes even more obvious. The Joint and Combined Warfighting School is the primary means for officers to receive Phase II, yet less than 40 percent of those attending are en route to, or in the first year of, their initial joint assignment. Additionally, many of those attending have already completed their first or second joint tours. These JPME II graduates often lament that they "should have had this education before starting a joint assignment," while also stressing their expanded "understanding of the similarities and differences between Service and interagency cultures" after completing the course.[22] Given that many, if not most, officers receive only a single joint assignment during their career, delivering JPME II to them at the end of their tour or afterward is akin to a physician attending medical school only after completing his or her practice.

Senior Airmen conduct survival training at U.S. Army's Jungle Operations Training Course in Hawaii, March 7, 2017 (U.S. Air National Guard/Christopher S. Muncy)

Here again, the accreditation of the Service war colleges may have aggravated the situation because the Services have historically viewed JPME II in terms of its requirement for promotion to general or flag officer rather than its preparatory value.[23] In this way, it makes more sense for an officer to receive JPME II credit while attending a war college when such a promotion is more likely and proximate. The legislative changes in 2007 also allow Service personnel managers to withhold officers from receiving JPME II until attendance to a senior Service college rather than in advance of a joint assignment. When attendance to a JPME II–accredited senior-level college is not possible, the Services often send these senior officers to the Joint Forces Staff College (JFSC) with the effect of preventing other more junior officers from attending.[24]

Overlooking the purpose of JPME II and its preparatory nature present considerable obstacles to improving the effectiveness of the joint force. Joint preparation necessitates joint acculturation, and the two must occur simultaneously to achieve the goal of improving the joint force and fulfill the intent of Goldwater-Nichols. Our joint warfighters deserve the investment in jointness, which is an investment in our success.

Fulfilling the Intent of Goldwater-Nichols and the Skelton Panel

The security challenges facing the Nation in the 21st century require its military force to possess an unprec-

Marines with 2nd Reconnaissance Battalion, 2nd Marine Division, II Marine Expeditionary Force, during reconnaissance mission at Onslow Beach, North Carolina, in support of exercise Bold Alligator 14, November 4, 2014 (U.S. Marine Corps/Paul Peterson)

edented level of lethality, flexibility, and resilience. Yet it is difficult to imagine how it might achieve such excellence without deepening and broadening the degree of jointness that presently exists in the joint force. Joint attitudes and perspectives and the interpersonal trust these enable are essential to achieving the highest degree of coordination and comprehensive integration of Service competencies and capabilities during conflict. Indeed, trust is what binds the joint force together, so DOD must return to and refocus on the development of this most important mental aspect of modern joint warfighting.[25] The mental aspect of joint development endures as the intent of the reforms to joint education made more than 30 years ago, and it has only become greater and more urgent as the demand for joint effectiveness increases.

While commanding U.S. Joint Forces Command, General Mattis routinely stated that "jointness is not a natural state," meaning that Service parochialism will slowly and ultimately erode any gains in jointness without continuous external pressure driving the Services to be interdependent.[26] This external pressure, however, has slowly and steadily ebbed in the last two decades. While most would espouse the importance of jointness and the need for quality joint education to cultivate the attendant attitudes and perspectives, in practice this has not been the case. The accreditation of a multitude of JPME II programs, each with a different mission, structure, and approach, has obscured the principal purpose of JPME II. Without standardization of joint acculturation approaches and objective measurement of acculturation outcomes, accredited institutions are free to make what they want of JPME II. In this regard, it will be difficult (but not impossible) for DOD to establish a common JPME II standard in the OPMEP that all institutions will willingly meet to gain and preserve accreditation. However, it is a necessary endeavor if this phase of joint education is to again achieve the principal purpose envisioned by the Skelton Panel. At the same time, it must assess the effectiveness of JPME II programs by objectively measuring the joint acculturation outcomes. Without this assessment, it remains unknown whether graduates are substantially more joint-minded as a result of attending Phase II. Currently, the Joint Staff is indeed exploring how it might perform such an assessment across the various accredited JPME II programs, but this effort will require unwavering dedication and considerable time if it is to be successful.

Standardization and assessment of existing JPME II approaches to achieve joint acculturation, to a degree that is prudent and meaningful in the joint operational environment, will take time and resources—it cannot be accomplished quickly or cheaply. DOD must invest in qualitative rather than quantitative outcomes for joint education, and it must be vigilant in guarding against the "diploma mill" approaches to JPME II of which the Skelton Panel warned.[27] But if officers continue to receive joint education at the wrong time, there will

be a limit to the advancement of jointness and benefit to the joint force, regardless of commonality in approaches and consistency in outcomes.

As flight school is the preparatory education for a pilot to take the controls of an aircraft, JPME II must be widely understood by DOD and the Services as the preparatory education for officers headed to their initial joint assignments. Short of reinstating the legislative requirement for such, DOD must substantially increase the pressure placed on the Services, and their personnel managers, to send officers to JPME II *prior to* their first joint assignment. This means the Services and joint commands must reconcile who "eats" the time that the officer is away from their duties for this important educational experience that enhances the likelihood for a successful joint assignment. Only in this way will attendance to JPME II be seen as less of a requirement for promotion to general or flag officer and more as a means to improve the effectiveness of the joint force. Through a "right officer, right time" approach, by providing Phase II to officers who actually need it, DOD will achieve not only greater cost-effectiveness in joint education but also greater joint efficacy through officers who can overcome the disproportionately steep learning curve associated with joint duty. Likewise, DOD must correspondingly invest in, *rather than divest from*, the capacity of the JPME II programs to accomplish this goal. Despite long-held concerns that existing JPME II alternatives fall short of the throughput needed to accommodate the number of officers rotating into joint assignments annually, DOD has allowed the capacity to erode. Though JFSC produces more than half of all JPME II graduates, cuts to faculty have diminished its annual throughput by almost 25 percent in recent years.

When the Skelton Panel conceptualized JPME II, its explicit and paramount intent was for the cornerstone for any JPME II program to inculcate greater understanding and appreciation for Service cultures, so that in the minds of students they could trust in their fellow Servicemembers. Congressman Skelton understood the value of joint acculturation in enabling officers to reject "approaches that always favor their own Service" and to inspire "mutual trust and confidence."[28] Though the reforms to joint education are now more than three decades old, joint education, and JPME II in particular, has never been more important as it is now for the success of the joint force. It cannot achieve the lethality, flexibility, and resilience sought by the current defense strategy through acquisition of platforms and technical capabilities alone. Indeed, platforms and advanced technologies are not even the most important investments. Rather, DOD must aggressively educate the joint force to cultivate greater and broader intellectual capacity if it is to apply those acquisitions with optimal joint effectiveness. The future of our joint force is at stake. **JFQ**

Notes

[1] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 8, available at <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[2] House Armed Services Committee, *Report of the Panel on Military Education*, 101st Cong., 1st sess., April 21, 1989, 105, available at <www.au.af.mil/au/awc/awcgate/congress/skelton1989/skelton.pdf>.

[3] Martin E. Dempsey, *Joint Education White Paper* (Washington, DC: The Joint Staff, July 16, 2012), 3–4.

[4] House Armed Services Committee, Subcommittee on Oversight and Investigations, *Another Crossroads? Professional Military Education Two Decades after the Goldwater-Nichols Act and the Skelton Panel*, April 2010, 167, available at <www.dtic.mil/dtic/tr/fulltext/u2/a520452.pdf>.

[5] *Report of the Panel on Military Education*, 57.

[6] Ibid., 4, 64, 127.

[7] Though the report of the Skelton Panel did not explicitly reference social science literature concerning acculturation and attitudinal change, there remains substantive and substantial support in the field for the panel's approach to achieving the desired joint attitudes and perspective. Foremost among this support is the literature on Intergroup Contact Theory and the acculturation research of D.L. Sam and J.W. Berry.

[8] *Report of the Panel on Military Education*, 102, 105.

[9] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3500.01H, *Joint Training Policy for the Armed Forces of the United States* (Washington, DC: The Joint Staff, 2014), A-4.

[10] *Another Crossroads?* xii.

[11] Title 10, *U.S. Code* § 2155, "Joint Professional Military Education Phase II Program of Instruction," prescribes host Service representation may not exceed 60 percent, with the remaining Services proportionally represented; even in the best case, such programs remain largely Service-centric in terms of students, faculty, curriculum, and surroundings, and the absence of a culturally neutral setting hinders acculturation.

[12] *Report of the Panel on Military Education*, 97–99.

[13] *Another Crossroads?* 65; See also Public Law 101-189, *National Defense Authorization Act for Fiscal Years 1990 and 1991*, § 1122, "Clarification Regarding Schools That Are Joint Professional Military Education Schools for Purposes of Qualification of Officers for Joint Specialty."

[14] CJCSI 1800.01E, *Officer Professional Military Education Policy* (Washington, DC: The Joint Staff, May 29, 2015), E-H-1.

[15] Ibid., E-1.

[16] Ibid., B-2–B-3.

[17] This Process for Accreditation of Joint Education (PAJE) assessment is derived from the authors' participation on multiple accreditation and staff assistance visits as well as selected Joint Staff J7 PAJE reports.

[18] DOD Instruction 1300.19, *DOD Joint Officer Management (JOM) Program* (Washington, DC: Office of the Secretary of Defense, March 4, 2014), 16–17; *Another Crossroads?* 22.

[19] *The Joint Staff Officer Project*, Final Report (Washington, DC: The Joint Staff, April 2008), 10.

[20] *Another Crossroads?* xiv.

[21] *The Joint Staff Officer Project*, 25.

[22] These comments are repeatedly observed in the end-of-course survey responses by students attending the JPME II programs at the Joint Forces Staff College.

[23] *Another Crossroads?* xii; see also Vincent C. Bowhers, "Manage or Educate: Fulfilling the Purpose of Joint Professional Military Education," *Joint Force Quarterly* 67 (4th Quarter 2012).

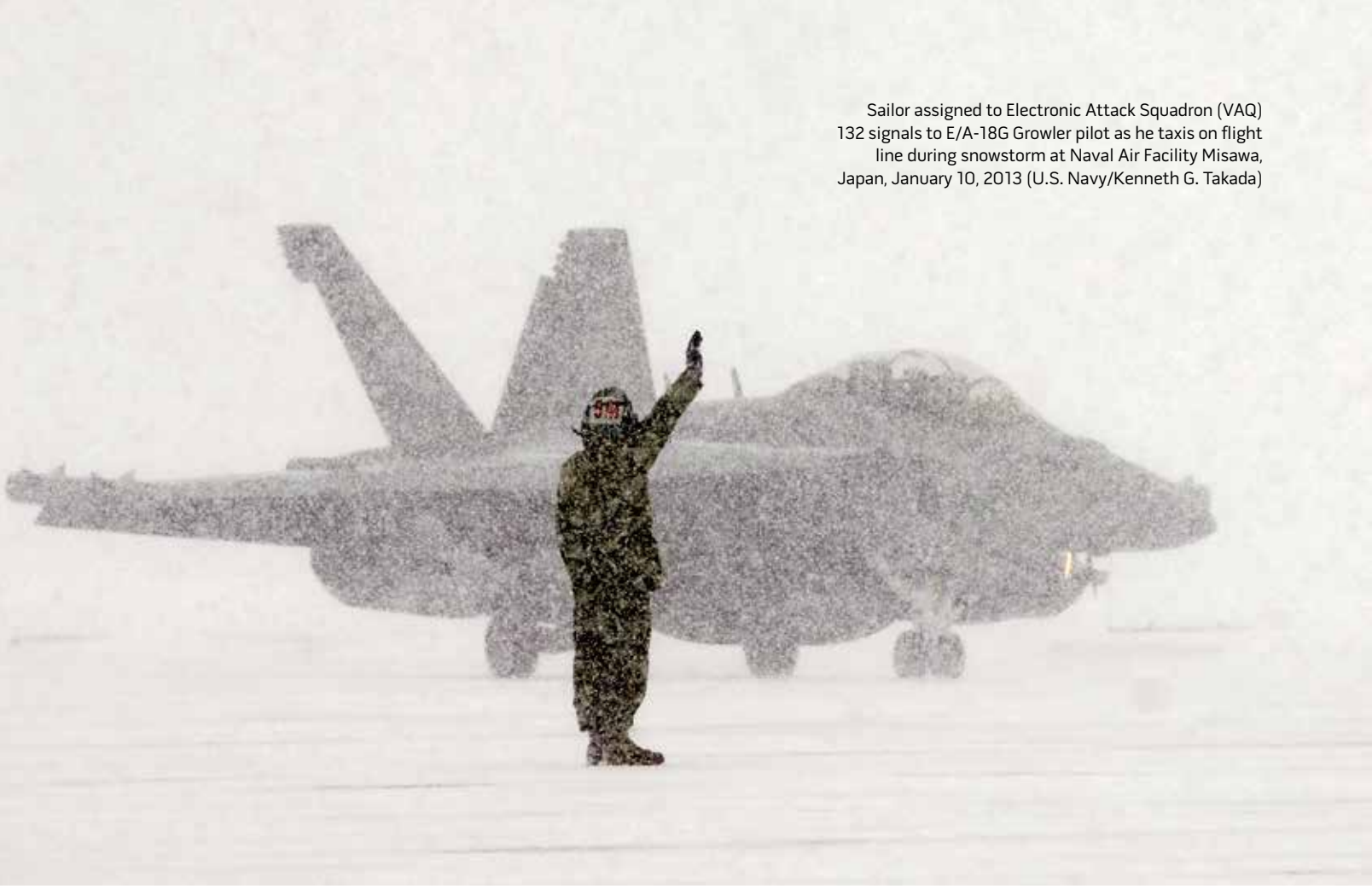
[24] *The Joint Staff Officer Project*, 69.

[25] Martin E. Dempsey, *Mission Command* (Washington, DC: The Joint Staff, 2012), 6; see also Les Brownlee and Peter J. Schoomaker, "Serving a Nation at War: A Campaign Quality Army with Joint and Expeditionary Capabilities," *Parameters* 34, no. 2 (Summer 2004), 11.

[26] "Command Briefing," U.S. Joint Forces Command, Norfolk, VA, June 2010.

[27] *Report of the Panel on Military Education*, 112.

[28] Ibid., 55.



Sailor assigned to Electronic Attack Squadron (VAQ) 132 signals to E/A-18G Growler pilot as he taxis on flight line during snowstorm at Naval Air Facility Misawa, Japan, January 10, 2013 (U.S. Navy/Kenneth G. Takada)

Simplicity

A Tool for Working with Complexity and Chaos

By Dale C. Eikmeier

If you can't explain it simply, you don't understand it well enough.

—Anonymous

A good plan, violently executed now, is better than a perfect plan next week.

—General George S. Patton

Dale C. Eikmeier is an Assistant Professor in the Department of Joint, Interagency, and Multinational Operations at the U.S. Army Command and General Staff College.

In comedian Don Novello's satirical skit "The Five Minute University," Father Guido Sarducci offered college degrees after completing a 5-minute curriculum.[1] The premise is only to teach what one could recall 5 years later because more than that was a waste of time and money. Thus, the economics course was "supply and demand," and business was "buy low and sell high." The skit was a huge hit, especially among university audiences. Novello capitalized on human nature's need to simplify complexity by reducing its key components to reasonably accurate "rules of thumb." These simple rules help facilitate informed, timely, and acceptable problem-solving and decisionmaking.[2]

Rules of thumb like supply and demand are heuristics that enable reasonably good decisionmaking without the time-consuming and occasionally paralyzing need to understand all the complexities and nuances of a situation.[3]

The fact is the "benefits of such heuristics are not only that they reduce complex information to a simple and manageable set of choices [but that] they [also] help people turn an intention into a realized action."[4] A good heuristic simplifies complexity by providing a "manageable set of choices" for taking action. Therefore, they are powerful tools that counter "paralysis by analysis" and procrastination and enable leaders to think and decide more quickly thus getting ahead of a competitor's decision cycle.

Why Heuristics and Simplification

Why are heuristics and simplification worth discussing? Because the joint force is looking for "better ways to develop agile and adaptive leaders who can operate in the complex and chaotic environment the Army [and joint force] expects for future conflicts."[5] Heuristics, especially acronym heuristics, and simplification can play important roles in promoting agile thinking. Unfortunately, the current doctrinal approach to this challenge is to add complexity on top of complexity in a quixotic quest for true understanding. Antoinette Schoar in "The Power of Heuristics" states:

The typical program aims to counter the inherent complexity of the decision by providing in-depth information. By providing such extremely detailed and complex information, these interventions try to enable people to make perfect decisions. For example, in the aftermath of the financial crisis in the United States, some policymakers suggested that individual savers should be taught about the complexities of interest rate models, portfolio allocation, and so on. . . . Everywhere, policy seeks to improve complex decisions by providing people with commensurately complex information.[6]

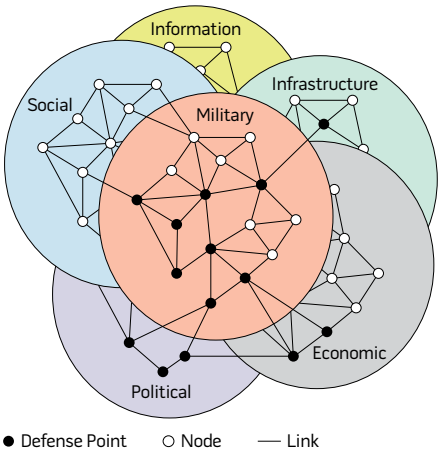
An example of adding "commensurately [more] complex information" are discussions in military forums of using quantum mechanics as a way to improve our understanding of complex environments.[7] However, Milan Vego argues against adding more complexity in his article "The Bureaucratization of the U.S. Military Decisionmaking Process." He states, "Since the early 1990s, the trend has been to progressively clutter each step of the estimate with poorly related or even unrelated considerations. This in turn has made the decisionmaking process cumbersome, rigid, and time-consuming."[8] So rather than creating agile and adaptive leaders capable of timely decisions, doctrine is having the opposite effect by exacerbating the complexity problem and unintentionally promoting decisionmaking paralysis.

An example of this "clutter" is the Joint Publication (JP) 5-0, *Joint Planning*, replacement of the 2011 JP 5-0 figure III-5 (figure 1) with figure IV-5 (figure 2).[9] The latter figure, "Holistic View of the Operational Environment," contains approximately 27 to 29 elements. The intent is to capture just about everything that makes up the operational environment. By contrast, the 2011 figure is quite simple, containing only six factors: political, military, economic, social, information, and infrastructure, collectively known as PMESII.

The question is which figure contributes to better understanding the environment and decisionmaking: the figure with close to 30 factors, that no one will recall, or the one with 6 easily recalled factors that is probably a "good enough" framework for describing the environment? A generation of military professionals, when asked to describe the operational environment, will quickly recall and frame their answer using PMESII, a "recognition" heuristic, and their description, while not perfect, will be acceptable. On the other hand, the 2017 figure IV-5 generation may have difficulty recalling anything other than a Rubik's Cube and will probably struggle to start.

A component of the quest for agile and adaptive leaders should include simplification and the expanded use of heuristics that enable leaders to make decisions faster and move forward in the face of overwhelming complexity and chaos. Like battle-drills or emergency procedures, heuristics such as "Aviate, Navigate, Communicate" jumpstart the decisionmaking process, enabling quicker action in the face of chaos and complexity.

Figure 1. Political, Military, Economic, Social, Information, and Infrastructure Systems Analysis



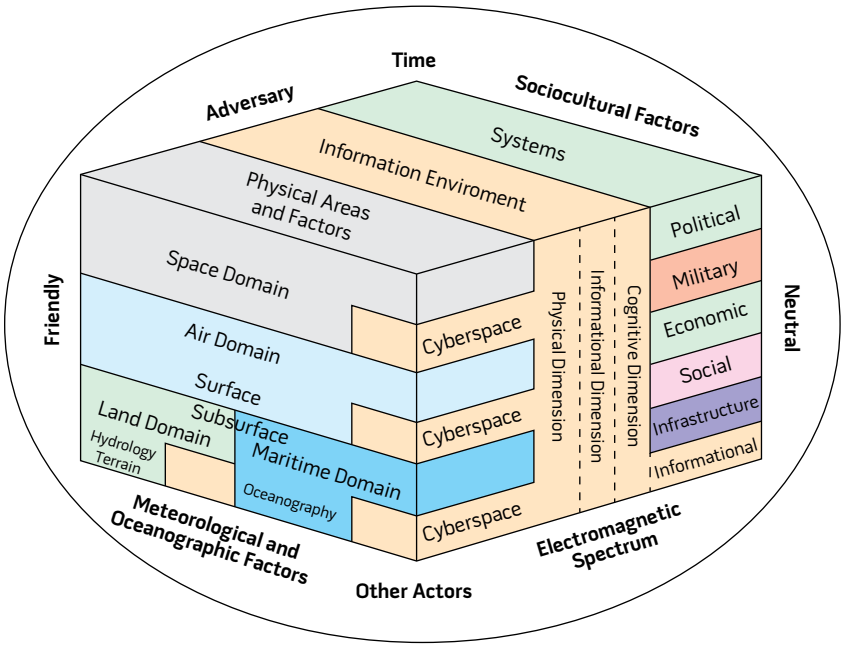
The Science of Heuristics and Simplification

There are two types of heuristics. First is the recognition or "availability" heuristic that aids problem-solving and decisionmaking by making already stored information more easily recalled. The second is the "representative" heuristic that aids decisionmaking by providing a mental prototype to compare with the current situation.[10] More simply, one recalls, and the other provides a model for comparison.

So how do heuristics actually work? Behavioral scientists and psychologists identified three factors that affect our decisionmaking process: limited memory, complexity-induced procrastination, and distraction caused by information overload.[11]

Psychologists confirmed that simplified and bundled information is more easily absorbed, recalled, and acted on because, beyond a certain level, the mind ignores complex information. Scientists discovered that the most successful students group long bits of information into manageable, easily recalled bundles. An example is the way we group a series of digits. For example, we say, "In the year fourteen ninety-two," two easily remembered digits, rather than, "In the year one thousand, four hundred, and ninety-two." Or rather than understanding

Figure 2. Holistic View of the Operational Environment



and explaining the complexity of market variables, commodities, and supply chains, we explain a change in commodity prices by "supply and demand." Two words joined by a conjunction. The conclusion is that "a single, easy-to-remember rule—a recognition heuristic—is more likely to be recalled and thus acted upon than a complex explanation of the underlying theory."[12] Thus, in a crisis one is more likely to recall and rely on a simple rule of thumb—a representative heuristic—rather than a time-consuming detailed analysis of the exact situation. The classic example is the "fight or flight" process—an instinctive heuristic.

Behavioral scientists also found that complexity causes procrastination regardless of how important the task is. This is why most people file tax returns at the last moment. Complexity overwhelms and people often do not know how or where to begin. However, when provided with simple rules, such as "stop, drop, and roll," scientists found that the likelihood of task completion increased.[13] So when faced with seemingly complex problems, often all that is needed is a framework or a model—the representative heuristic—to help jumpstart the problem-solving and decisionmaking process. Whereas complicating decisionmaking by adding more complex lists, steps, factors, and considerations of environmental understanding actually slows the process. Rather than focusing on solving the problem, we let the process capture us.

The third factor is overload caused by too much information. Studies have shown that "Having a lot of secondary information 'clutter' obscures key information and makes people less likely to grasp and absorb the key message."[14] A possible solution to limited memory, complexity-induced procrastination, and information overload is *less*, not more.

The Advantages of Simplicity

To better achieve understanding in complex environments, evolving doctrine believes more is the key. This leads to the addition of processes, lengthy checklists, and an ever-increasing number of steps and substeps. According to Professor Vego, this quest for better understanding has obscured the original intent and distinctions between estimates, planning, and decisionmaking—and prioritized format over process.[15] This clutter drives the need for longer complex checklists and unwittingly creates a blind "check the block" mentality devoid of holistic and critical thinking. What decisionmakers and planners need is more simplification, or rules of thumb, because simplification clears the clutter and feeds clarity, and clarity enables sound and timely decisionmaking.

A study at the Army's Command and General Staff College titled "The Effect of Simple Role-Playing Games on the Wargaming Step of the Military Decision Making Process (MDMP): A Mixed Methods Approach" reinforced the value of simplification. In this study, students using a relatively simple war game learned to employ those visualization skills in a complex war game more effectively than a control group. The researchers, led by Dr. Richard McConnell, concluded:

this study suggests that there is a correlation between playing simple role-playing games such as Kriegspiel [a 19th-century Prussian game], *which would then make planners more effective at Course of Action Analysis (wargaming) during the Military Decision Making Process (MDMP). Specifically, participants who played Kriegspiel demonstrated a statistically significant increased capability to see themselves in the context of their operational environment while addressing threats and opportunities and integrating those discoveries across war fighting functions.*[16]

They found that playing the simple Kriegspiel game first provided the students some useful mental tools that contributed to better visualization and execution during the much more complex course of action analysis in military planning. In other words, experience gained with a simple application provided insights that enabled a higher level of performance in a more complex application.

This suggests that experience with simple processes first, combined with rules of thumb (insights), can help overcome complexity-induced procrastination, memory limitations, and information distraction in more complex processes, thus enabling higher performance when dealing with complexity and chaos.

Sailor prepares to mark location of simulated casualty on damage control plates during general quarters drill aboard USS *Dewey* during RIMPAC exercise, July 14, 2018 (U.S. Navy/Devin M. Langer)

Cautions and Limitations

Heuristics and simplification have their limitations. Daniel Kahneman, in his book *Thinking Fast and Slow*, argues, "In general, these heuristics are quite useful, but sometimes they lead to severe and systematic errors."[17] Any unthinking use of heuristics, especially representative heuristics, can lead to bias resulting in poor judgments and stereotyping. Kahneman goes on to state, "A better understanding of these heuristics and of the biases to which they lead could improve judgments and decisions in situations of uncertainty."[18] The key to using heuristics wisely is understanding their potential for bias and using critical thinking to overcome it. Combining these can inoculate the user against "severe and systematic errors."

The other limitation is potential simplification of what is *not* simple.[19] If time permits, and a detailed study of a complex situation is important to sound decisionmaking, then use heuristics cautiously and continually review their applicability to the situation. Jacob Mong of the Command and General Staff College cautioned, "we need to be vigilant in that those heuristics must be re-examined, challenged, and adjusted to fit individual situations. So, treat the acronyms and mnemonics as a start point/first try, then re-evaluate/assess, and adjust accordingly."[20]

Acronyms as Powerful Heuristics

Acronyms are recognition heuristics that enable us to simplify the complex, absorb key elements, and quickly recall them so that we can move forward. They help provide simple rules of thumb or frameworks that can combat limited memory, procrastination, and information overload.

Acronyms used as recognition heuristics have two functions: storage and recall. First, they create a framework that helps label and categorize new information. Second, they then serve as a search engine helping to recall the stored information. For example, inexperienced platoon leaders using the acronym of METT-C (mission, enemy, troops, terrain and time, and civilians) can quickly grasp and recall the complexities of the combat environment and take action. OCOKA (observation, cover and concealment, obstacles, key terrain, and avenues of approach) is another example that captures the complexity and nuance of the physical environment. Without the use of these acronyms, the education of new officers would be more difficult and their performance in the field would arguably suffer from complexity procrastination.

At a higher level, the acronym DIME (diplomacy, information, military, and economics) frames and captures in a simple but powerful way the complexities of international power. However, for some, DIME was too simple. Following the natural trend to increase complexity, there was a short-lived attempt in the early 2000s to make DIME more descriptive and complete. DIME-FIL added finance, infrastructure, and legal.

Stinger missile team with 35th Air Defense Artillery Brigade identifies unmanned aerial vehicle target during RIMPAC 2018 at Pacific Missile Range Facility, Barking Sands, Hawaii, July 24, 2018 (U.S. Army/Adan Cazarez)

Then there was MIDLIFE (military, information/intelligence, diplomatic, legal, infrastructure, finance, and economic). Common sense prevailed and, in the end, a simple four-letter word won.

The Army added "physical environment and time," for PMESII-PT, to joint doctrine's PMESII. This is probably acceptable because it does not violate memory limitation or information clutter, unlike JP 5-0 figure IV-5. However, the Army needs to be wary of the bureaucracy's tendency to add more letters. Is a "C" for cyber lurking out there?

Some Nondoctrinal Heurisics

According to JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, having a system's perspective is critical to understanding the operational environment (OE).[21] However, recognizing and describing a system can be challenging, especially if one does not have tens of hours of instruction in systems theory. The Army's Command and General Staff Office's Course (CGSOC), not having hours of curriculum time for systems theory, used the Five Minute University model and managed to successfully teach systems theory using the acronym RAFT (relationships, actors, functions, and tensions). It is systems theory's equivalent of supply and demand for economics. Easily understood and recalled, RAFT jumpstarts the understanding and description of systems.

In RAFT, an environment is comprised of various systems or subsystems called "actors" (also referred to as nodes). Each actor has "relationships" to other actors (also referred to as links). These relationships between actors serve some purpose, which is the "function." Functions are typically verbs, such as supply, control, or feed. "T" is for tension, and it is a characterization of the relationship/function. Tensions are typically adjectives, such as strong, required, positive, negative, or adversarial.

Using RAFT, CGSOC students are able to quickly chart and describe environments to an adequate level of detail for use in operational design and the joint planning process. They then identify the key actors and their relationships. These become decisive points, or "high points of leverage," that indicate where and what types of action may be appropriate. This becomes the outline of an operational approach or solution to a problem. Technically, a more accurate acronym would be ARFC (actors, relationships, functions, and characterizations) because it better describes the sequence of the process. However, it is cognitively weaker. Acronyms that use existing words, such as DIME or RAFT, which already reside in the mind, make filing and recall easier. Therefore, we use RAFT, not ARFC.

Another example is RCP (remove, change, and provide), which is a framework for problem-solving, and planners use it in the development of a broad operational approach during the operational design process. Just about any problem and solution can be reduced to the rule of thumb "remove, change, and provide." If something in the environment causes the problem, remove it. If it is a required part or cannot be removed, then change its behavior. Alternatively, if the problem is that something is missing, provide it. For problems that are

more complex, combinations of RCP may work. For example, if the problem is crime, remove criminals, change the behavior of people to reduce crime, and provide opportunities other than crime. Again, it is a simple rule of thumb to help start the problem-solving process.

Conclusion

The scientific opinion of many psychologists and behavioral scientists suggests the key to time-sensitive decisionmaking in complex and chaotic situations is simplicity, not complexity. Simple-to-remember rules of thumb, or heuristics, speed the cognitive process, enabling faster decisionmaking and action. Recognizing that heuristics have limitations and are not a substitute for basic research and analysis, they nevertheless help break complexity-induced paralysis and support the development of good plans that can achieve timely and acceptable results.

The best heuristics capture useful information in an intuitive, easy-to-recall way. Their utility is in assisting decisionmakers in complex and chaotic situations to make better and timelier decisions that lead to effective actions. While tested and vetted heuristics provide opportunities to create better ways to pass and retain knowledge and skills, designers must ensure that they capture reliable best practices.[22]

Leaders and doctrine writers seeking to enable better decisionmaking and situational awareness should seriously consider taking a new direction toward simplification of processes. Rather than adding more to already bloated and complex processes, they should answer three questions: First, does this add or reduce clutter? Second, does this complicate or simplify understanding? Last, is it forgettable or memorable? If the answers are the former then consider cutting and simplifying by using reasonable heuristics. **JFQ**

Notes

[1] Father Guido Sarducci (Don Novello), "Five Minute University," available at <www.templaruniversity.com/guido.html>.

[2] Kendra Cherry, "What Is a Heuristic and How Does It Work?" *VeryWellMind.com*, November 13, 2018, available at <www.verywellmind.com/what-is-a-heuristic-2795235>.

[3] Antoinette Schoar and Saugato Datta, "The Power of Heuristics," *Ideas42.org*, January 2014, 2, available at <www.ideas42.org/wp-content/uploads/2015/05/ideas42_The-Power-of-Heuristics-2014-1.pdf>.

[4] Ibid.

[5] David Vergun, "Solarioum 2015: Developing Agile, Adaptive Leaders," *Army.mil*, available at <www.army.mil/article/143630/solarium_2015_developing_agile_adaptive_leaders>.

[6] Schoar and Datta, "The Power of Heuristics," 2.

[7] Grant M. Martin, "Carl von Clausewitz, Meet Albert Einstein and Max Planck," *Small Wars Journal*, n.d., available at <http://smallwarsjournal.com/index.php/jrnl/art/carl-von-clausewitz-meet-albert-einstein-and-max-planck>.

[8] Milan Vego, "The Bureaucratization of the U.S. Military Decisionmaking Process," *Joint Force Quarterly* 88 (1st Quarter 2018), 35.

[9] Joint Publication (JP) 5-0, *Joint Planning* (Washington DC: The Joint Staff, June 2017), IV-12; and JP 5-0, *Joint Operational Planning* (Washington DC: The Joint Staff, August 2011), III-10.

[10] Cherry, "What Is a Heuristic and How Does It Work?"; and Daniel G. Goldstein and Gerd Gigerenzer, "Models of Ecological Rationality: The Recognition Heuristic," *Psychological Review* 109, no. 1 (2002), 75–90, available at <www.dangoldstein.com/papers/RecognitionPsychReview.pdf>.

[11] Schoar and Datta, "The Power of Heuristics," 3.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Vego, "The Bureaucratization of the U.S. Military Decisionmaking Process."

[16] Richard A. McConnell et al., "The Effect of Simple Role-Playing Games on the Wargaming Step of the Military Decision Making Process (MDMP): A Mixed Methods Approach," *Developments in Business Simulation and Experiential Learning*, vol. 45 (2018), 340.

[17] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 419.

[18] Ibid., 431.

[19] Cherry, "What Is a Heuristic and How Does It Work?"; and Goldstein and Gigernzer, "Models of Ecological Rationality."

[20] Jacob Mong, email to author, "Subject: Quote from Your Recent Study, 10 April 2018."

[21] JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment* (Washington DC: The Joint Staff, May 2014), I-4.

[22] Schoar and Datta, "The Power of Heuristics," 6.

Airman guards B-52 Stratofortress during U.S. Strategic Command exercise Global Thunder 2019 at Barksdale Air Force Base, Louisiana, November 2, 2018 (U.S. Air Force/ Mozer Da Cunha)

"This Breaking News Just In, Emperor Napoleon I Is *Still* Dead!"

By John M. Fawcett, Jr.

We need to look at whether the military is fundamentally structured to meet both old and new challenges.

—Senator John McCain

The challenges of the National Security Strategy and National Defense Strategy provide an opportunity to examine the U.S. military in order to provide a more agile and flexible force, leveraging partnerships to provide defense of the homeland and force projection capability for warfighting as well as responses to natural and man-made disasters. These challenges are not unique to our most recent strategic guidance. In November of 2014, Secretary of Defense Chuck Hagel outlined the challenges facing the U.S. military.[1] Secretary Ashton Carter continued this theme in a fireside chat at West Point in March 2016,[2] as did his successor James Mattis in statements published in 2017.[3] This article focuses on one aspect of the challenges and discussions: the combat-

Lieutenant Colonel John M. Fawcett, Jr., USAF (Ret.), is Deputy Branch Chief at North American Aerospace Defense Command and U.S. Northern Command J533.

ant command (CCMD) organization for command and control (C2) of U.S. military forces.

CCMDs provide both theater security cooperation (TSC) and warfighting response as well as key functional capabilities. Any proposed changes must operate within the framework of TSC and warfighting, including the ability to create and command appropriate subordinate organizations in response to natural or man-made crises. There are three options for moving forward with theater command and control. The first is to do nothing. In a period of resizing and recapitalizing the force in conjunction with constrained budgets, this is the most likely option, but the least effective in terms of incorporating lessons learned over the last two decades of conflict and the projections of where conflict will occur in coming decades. Option two is to modify the existing structure, but keep it basically intact. Previous attempts at this option have resulted in shifting without substantive change. Staffs have been reduced by target numbers arrived at by political agreement in the Pentagon and not a rational approach to missions and tasks. Ultimately, staff directorates at the theater commands are reduced by a "fair sharing" of the targeted cuts. There is a third option found in an opportunity to rationalize the command and component structure. The theater C2 structure could be approached from a new angle, examining events in Southwest Asia as well as projected engagements in an enduring global conflict. This article addresses the third option.

Background

Unified command over U.S. operational forces was adopted in the European theater during World War II. While the United States was able to achieve a degree of unified command in the European theater under General Dwight D. Eisenhower, attempts to establish a single unified command for the Army and Navy in the Pacific theater proved impossible.[4] Today, there are six geographic CCMDs (GCCs) and four functional CCMDs (FCCs). The GCCs operate in clearly delineated areas of responsibility (AORs) and provide a distinctive regional military focus. The GCCs are U.S. Africa Command (USAFRICOM), U.S. Central Command (USCENTCOM), U.S. European Command (USEUCOM), U.S. Northern Command (USNORTHCOM), U.S. Indo-Pacific Command, and U.S. Southern Command (USSOUTHCOM). The FCCs operate worldwide across geographic boundaries and provide unique capabilities to GCCs and include U.S. Special Operations Command (USSOCOM), U.S. Strategic Command (USSTRATCOM), and U.S. Transportation Command (USTRANSCOM). U.S. Cyber Command (USCYBERCOM) has recently been elevated from a subunified command to full combatant command status.[5]

Each GCC focuses on planning and execution of tasked peacetime and wartime missions within its specific AOR. The combatant commanders (CCDRs) engage in TSC, training, and exercising with the military representatives of host nations in the AORs. Since U.S. tactical-level forces are large in absolute numbers, but small relative to the population base and the global range of missions, the regional knowledge and partnerships of the CCDRs and their staffs provide a key understanding of intelligence, surveillance, and reconnaissance (ISR) networks, joint intelligence preparation of the operational environment (JIPOE), and theater logistics and communications infrastructures.[6] Within their AORs, CCDRs have unique battlespace awareness that includes partners, allies, neutrals, potential adversaries, and the relationships among them that can inform operations.

The CCMD staff structure ostensibly creates the framework for engagement as well as long-term planning and crisis response. Other executive branch agencies, including the Department of State, Department of Justice, and Department of Homeland Security, are often collectively referred to as the interagency community and are involved to a greater or lesser degree depending on the command and mission. Since military tasks often intersect the responsibilities of these agencies, both FCCs and GCCs have integrated interagency representatives in their process structures to enhance operations. Examples of this integration include a State Department Deputy Commander for Civil-Military Activities at USAFRICOM; the Interagency Action Group established in the J3 directorate at USCENTCOM; the establishment of a J9 Directorate for Interagency Partnering at USPACOM, USSOUTHCOM, and USEUCOM; and a J9 that integrates and synchronizes the activities of civilian, state, Federal, and private-sector organizations at USNORTHCOM.[7]

What Is the Problem?

Distilled from documents ranging from the National Security Strategy, Unified Command Plan (UCP), Guidance for the Employment of the Force, and Joint Strategic Capabilities Plan, the GCCs have two significant missions: theater security cooperation and warfighting. Due to the policy commitment to a force with global requirements, the warfighting mission leverages the key partnerships of TSC, which may be construed as the most significant portion of military planning.[8] For example, humanitarian missions are not a funded responsibility for the Department of Defense (DOD), but are useful in creating strong relationships and an understanding of the AORs. Warfighting is another part of the range of military operations with unique skill sets devoted to direct action—killing people and breaking things. In addition, the current staff structure follows the European staff model with numbered sections or directorates, creating stovepiped staff organizations at the theater level and above. Successful commanders work hard to ensure cross staff communication and coordination.

Recent theater-level engagements of the U.S. military have reemphasized the importance of flexible teams at the theater-command level, able to both articulate long-term theater strategy and support tactical operations. In *Lessons Encountered: Learning from the Long War*, edited by Richard Hooker and

Joseph Collins, Dr. Collins provides an overview of the lack of clear military chain of command during initial operations in Afghanistan and Iraq during Operations *Enduring Freedom* and *Iraqi Freedom*. In Afghanistan, the transition from the Central Intelligence Agency and special operations forces (SOF) to more conventional operations was long and painful, resulting in confusion over goals, objectives, and endstates. Command and control in Iraq during the 2003 invasion was adequate, but the transition to post-invasion, steady-state operations created confusion. Multiple U.S. and coalition organizations and military commands were created. So while there is doctrine in place outlining the creation and use of joint task forces (JTFs), it appears this doctrine is followed in the exception rather than the rule, especially after cessation of hostilities.

Finally, exercises such as the Iron Crucible series have identified a problem with supporting multiple near-simultaneous crises in multiple GCC AORs. As the crisis response develops and creates demand for limited resources, there is no adjudication decisionmaker short of the Defense Secretary. Resource allocation has a gap between the CCMD capped planning process and the global perspective of the Joint Staff. For example, each of the theater four-stars may present a strong case for priority support for ISR, strategic lift, and specific force capabilities such as SOF. Currently, these demands tend to be solved informally between the GCC and FCC staffs. However, if there is an inability to reach consensus, the Secretary must decide. The existing process is also focused primarily on activity outside of the homeland and has little to no consideration for a strategic reserve. The homeland is no longer a sanctuary from conflict; therefore, a strategic reserve must be considered in case a natural or man-made disaster occurs in the homeland competing for limited DOD resources.[9]

Are There Existing Proposals?

RAND took on an evaluation of the Unified Command Plans in 1993 after the fall of the Soviet Union and prepared for the Army the *Evaluation Framework for Unified Command Plans: A Documented Briefing*. The evaluation does not fundamentally change the approach to combatant commands but provides a structure for evaluating alternative UCPs. The Center for Strategic and International Studies published *Beyond Goldwater-Nichols: Defense Reform for a New Strategic Era* as a three-phase report starting in 2004. The Phase I report focused on organizational changes at the DOD level, including the Service secretariats.[10] Phase II is more of the same, while the Phase III report looks at the Reserve component. There is little reference to the combatant commands. The current "Beyond Goldwater-Nichols" debate has tended to focus on the reduction of combatant commands, specifically combining some of the geographic commands, reducing the number of four-star positions, and mandating a reduction in theater-level and Service-component staffs.[11] For example, there is discussion about combining USNORTHCOM and USSOUTHCOM,[12] usually by people who fail to explain exactly how this combination, without a change in responsibilities, would be an improvement. Commands and components could also be standardized fairly easily around a structure of three-star component commanders of numbered Air forces, Army corps, Navy fleets, and Marine divisions. The current definitions of these component formations would have to be changed, but this modification is possible without significant legislative requirements. Both of these discussions tend to assume a similar geographic orientation and staff structure with a continuation of the two missions under the same commander.

One aspect of the current debate over changes to Goldwater-Nichols is the need to redefine theater-level command and control. In his 2013 paper on GCC command structures, Rhude Cherry III provides an overview of current command structures and modifications as well as a recommendation for a hybrid staff structure that creates military and civilian deputies while leveraging the existing staff structure.[13] There is also an *Insights and Best Practices Focus Paper on Geographic Combatant Commander Command and Control Organizational Options*, written by the Deployable Training Division of the Joint Staff J7 and published by the Joint Staff J7 Joint Training Directorate. This paper looks at the structure from the standpoint of existing doctrine while attempting to provide some improvements for JTFs and subunified commands.

The Congressional Research Service produced a report on January 3, 2013, titled *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*. As advertised in the title, the report provides a historical perspective of the evolution of the UCP and combatant commands and identifies questions that Congress may wish to ask during debate over future UCPs. These questions include the militarization of foreign policy due to the regional focus of the geographic combatant commands, the need for a whole-of-government approach to integrating the military in a larger policy framework, and whether or not there is a need for new functional or geographic commands. The report also looks at alternatives to combatant commands such as creating JTFs to replace the combatant commands or a joint interagency organization. While the report is an excellent overview and raises interesting questions, there are no substantive recommendations.

Alternative Structure Proposal

An alternative to the existing legacy is to divide the warfighting and TSC missions into two separate commands.

Geographic Commands. In this concept, the geographic-oriented approach is maintained, but the geographic commands (GCs) have a three-star commander responsible for all noncombat U.S. DOD interests in the AOR as well as a theater campaign plan or his portion of a global plan. This includes missions such as creating and assessing intelligence, logistics, and communications networks, and facilitating the TSC operations of training and exercising.

Effective cultural analysis and engagement will be at the heart of the GC. Cultural analysis is the creation of assessments on the different nation-states and nonstate actors in the AOR. Both the National Security Strategy and National Defense Strategy clearly state the importance of strategic partnerships as a way to increase military power.[14] The GC staffs and liaison officers (LNO) will be responsible for establishing personal relationships with military personnel in the AOR, and, when possible, personal contacts will be expanded to whole-of-government or whole-of-nation organizations. These relationships encompass both nation-state and nonstate actors in the AOR. Transnational organizations include the private sector and may be designated as criminal, noncriminal, or terrorists while stateless nations may be described as criminal or noncriminal or may be designated as terrorists.

As an example, Turkey (USEUCOM AOR) has a distinct culture that is oriented toward Europe and the Western philosophies of the Enlightenment and democracy, while retaining a distinct bias based on Islam that may run counter to generally accepted European cultural standards. The commander of USEUCOM must direct his staff to create cultural profiles for all the nation-states and stateless nations in his AOR, including Turkey. Since human interaction continues to define power relationships, the commander is *the* DOD face to the Turkish military, establishing the personal relationships that may be leveraged during crisis response to include combat operations. The commander must build these relationships through the TSC mission, as well as humanitarian relief. These same responsibilities will hold true for the other GCs. Service components for the GCs will be eliminated and the consolidation in a new structure will provide the necessary theater support.

Externally Focused Combatant Commands. With the GCs focused on the TSC mission, the execution of combat operations becomes the mission of one of three combat commands (CCs)—East, West, and Homeland—each with a four-star commander. East and West commands provide deployable command and control that will respond as required to crisis in the GCs' AORs and will have steady-state relationships with specific GCs. For example, East Command could support USOUTHCOM, USEUCOM, and USAFRICOM, while West Command could be tied to USPACOM and USCENTCOM.

Having two similar commands, East and West, provides for depth of trained personnel that could be shifted as required by actual operations in order to create the necessary JTF C2 structure. The CCs will be responsible for joint

Figure 1. Proposed C2 Structure (including integration of intelligence flow)

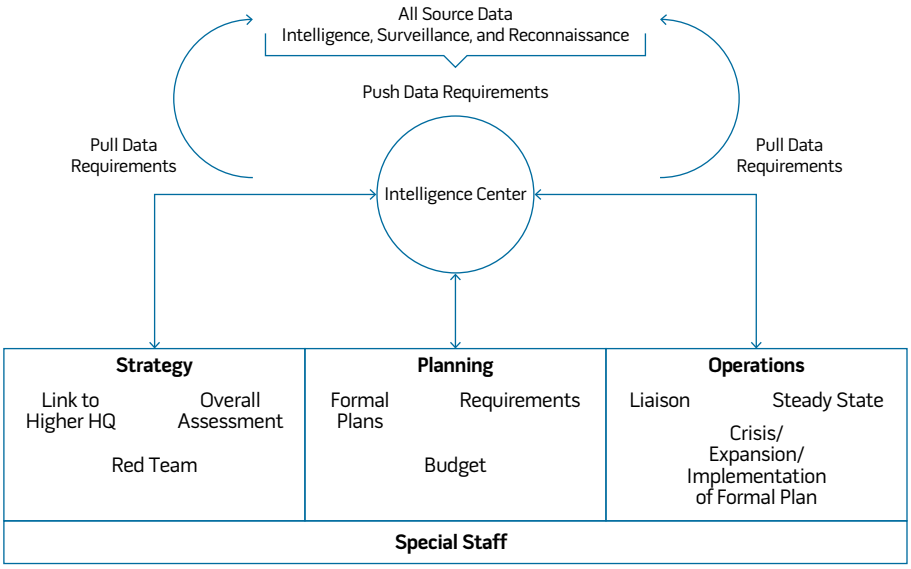
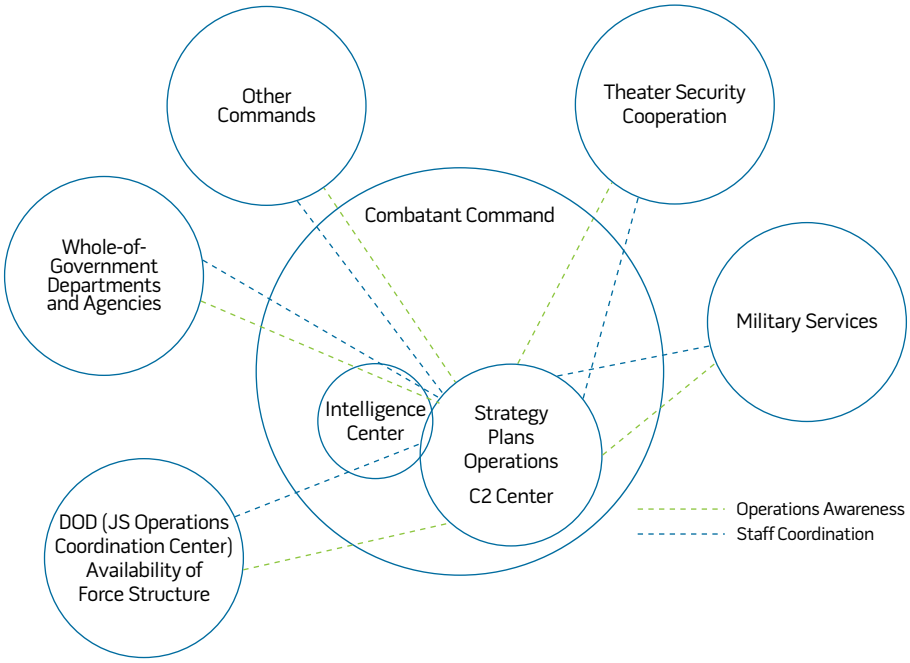


Figure 2. Combatant Command Steady State



Sailors rig barricade during drill on flight deck aboard *Nimitz*-class aircraft carrier USS *Harry S. Truman*, December 2, 2018, Mediterranean Sea (U.S. Navy/ Rebekah A. Watkins)

training, education, JTF-level exercises, and joint doctrine in support of the Chairman. With only two potential four-star "owners" of deployed task forces, adjudication of competition for limited resources is simplified.

The CCs are structured around three task areas: strategy, planning, and operations. There is also an Intelligence Center (IC) to develop the JIPOE and support combat operations. The IC will maintain constant contact with the ICs in the GCs. Figure 1 illustrates the construct, including the special staff. The traditional staff codes are eliminated, and the functional expertise is incorporated in the three major divisions of strategy, planning, and operations. The Special Staff includes functions such as the judge advocate general, public affairs, protocol, command surgeon, command chaplain, political-military advisor, Reserve and National Guard advisors, budget, knowledge management, and liaisons to other agencies.

A Red Team will establish and coordinate all training exercises and provide the Red, Blue, White, Gray, and Green perspectives for the crisis as well as feedback on the strategic message.[15] In short, the mandate for the Red Team is to provide a thinking enemy for assessment of plans and operations, leveraging the knowledge of the GC for the affected area.

The IC (former J2) has the daunting task of maintaining the constant flow and analysis of data as it streams in from classified and open sources, and fusing it into actionable intelligence. This is envisioned as a highly automated push and pull system, with the IC constantly combing through all sources and responding to analyst demands in support of commander requirements.

Figure 2 shows the C2 Center as the C2 node for the command, networked with the IC and the parallel C2 Centers in the GCs to maintain all-domain situational awareness. The three task areas and IC reflect observations by the author of theater and functional command activities over the last two decades. Figure 1 also arranges the process flows to reflect what happens with the C2 node for the command, supported by the rest of the staff during day-to-day operations.

The CCs will also have assigned Service components similar to the existing construct and will draw on these components to establish the JTF staffs. These components will be numbered Air forces, fleets, and corps, with three-star commanders, and Marine divisions commanded by a two-star. Each command will also have a SOF as well as a cyber component.

Further analysis may indicate the need for only one CC, increasing focus and overhead savings. Rather than East and

West combatant commands, there would be a Global Command. The Global Command could then mitigate the demands for scarce resources. Canada and the United Kingdom are currently using a single, globally oriented command structure. Canada has the Canadian Joint Operations Command and the United Kingdom has the Permanent Joint Force Headquarters. While both of these C2 arrangements have demonstrated their abilities on numerous occasions, an illustrative example is the British intervention in Sierra Leone between 2000 and 2002. The initial Operation *Palliser* required a rapid response while subsequent events, Operation *Barras* (a hostage rescue) and Operation *Silkman* (a commitment to train the Sierra Leone army), demanded continual British presence over the next 2 years, ultimately resulting in a stable situation.[16]

Homeland Command. Homeland Command (HC) will be a hybrid command combining aspects of both the GCs and CCs, responsible for response to natural and man-made disasters as well as combat operations. The four-star commander of HC will establish the necessary relationships with governments in the homeland and conform to the legal implications of the U.S. Constitution. The commander will be dual-hatted as the commander of North American Aerospace Defense Command and Homeland Command. HC will also have Service components: numbered air force, numbered corp, numbered fleet, and marine division, as well as SOF and cyber. With the establishment of HC, there will be a third four-star in the mix for resource competition, but internally focused.

Functional Combatant Commands. The FCCs will be assigned Service components. The National Security Agency will be assigned its own dedicated commander; the USCYBERCOM commander will not be dual-hatted. Eighth Air Force under USSTRATCOM will have operational control over bombers and land-based nuclear missiles, while Eighth Fleet will have operational control over nuclear missile equipped submarines. When resources are on alert, missiles, bombers, or submarines will be under the direct command of the USSTRATCOM commander. Due to the size of the Marine Corps and missions of the FCCs, only USSOCOM has an assigned Marine component headquarters. USTRANSCOM, USSPACECOM, USSOCOM, and USCYBERCOM may elect to put liaison cells in the command centers of the other FCs. The FCs may also assign liaison cells to the CCs.

If the proposal is adopted, even with two new externally oriented commands and the reestablishment of USSPACECOM, the number of four-stars is reduced from 17 to 10. These numbers include the current practice of four-star-led components, the problem of four-stars reporting to four-stars, and transitioning to no four-star components. Since every four-star comes with a commensurate staff, the reduction should pay for the manpower costs of the new commands at a minimum.

Figure 3. Geographic Command Warfighting Crisis Support Transition

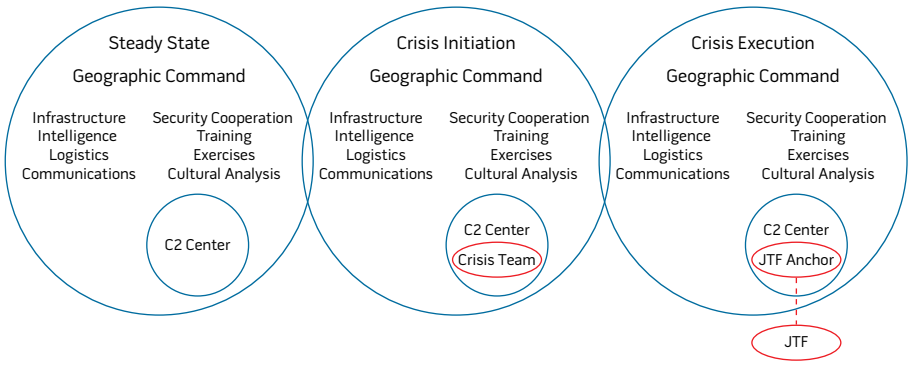
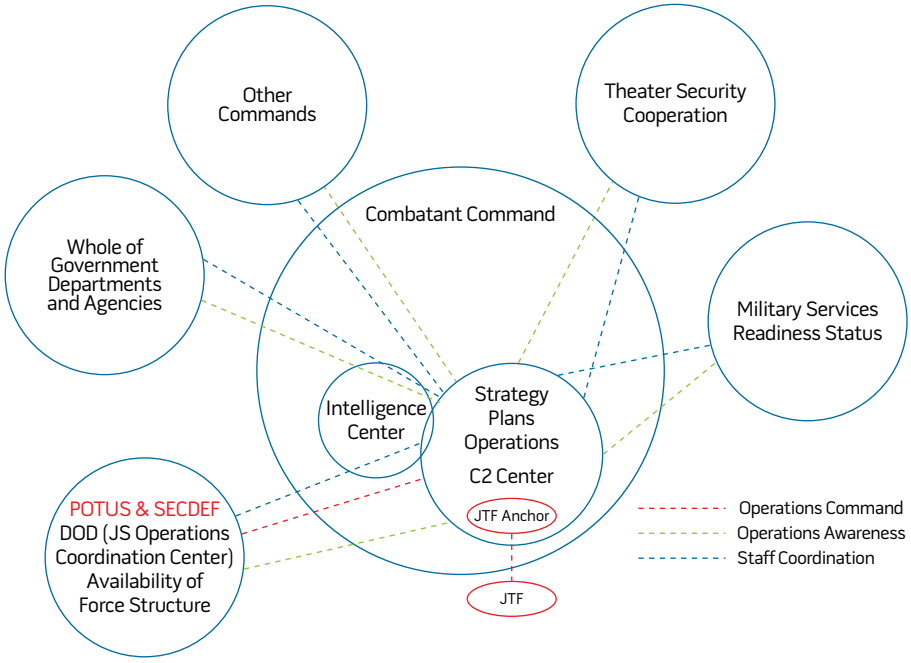


Figure 4. Combatant Command Crisis Execution



How It Works

The CC staff will form the nucleus of a JTF when required to respond to

a combat-related crisis. The JTF will start within the CC headquarters and expand by drawing on support from component, GC staff, and Service personnel. A designated JTF commander will assemble his or her staff for the assigned crisis, formulate the plans, and, if required, deploy to execute combat operations. The CC commander will maintain a strategy for the crisis consistent with the President's guidance in coordination with the Joint Staff and Secretary of Defense. CCs are not responsible for response to natural and man-made disasters since this problem set would be addressed by the GCs. The CCs will train and exercise on a regular basis to include the challenge of assembling JTFs.

The steady-state structure enables the CC to maintain day-to-day operational awareness and staff coordination across the Federal Government, the assigned GCs, and all relevant organizations. In addition, the planning staff will be responsible for formal plans within the AORs.

The Crisis Team is assembled in the C2 Center and begins updating plans and GC networks and assessments relevant to possible combat operations. The President and Secretary are now tied into the awareness network. The Crisis Team is expanded as required to prepare for deployment of a JTF to the affected area. Broad coordination across the executive and legislative branches of government is key to providing a globally consistent strategic message. The discipline of this coordination should also ensure that civilian leadership establishes clear political goals, objectives, and endstates for the crisis.

If the decision is made to proceed with force employment as part of the crisis execution, a JTF is deployed and assigned forces previously identified during the planning period between crisis initiation and crisis execution. The JTF commander builds a staff composed of previously identified and trained personnel from the CC, GC, and individual Services, and the Crisis Team transitions to support the JTF as the JTF anchor between the combatant commander and JTF commander (figure 3). JTF commanders will be certified one-, two-, and three-star officers who have completed JTF commander training. This training will consist of both initial certification and periodic updates, including participation in theater-level joint exercises, part of the CC's mission, to ensure commanders are prepared for combat operations. Only senior officers who are JTF commander qualified will be considered for the leadership of CCs and GCs. The staff of the CCs will exercise on a continuing basis using live, virtual, and constructive training programs to respond to a wide range of notional crises. GCs will participate in contingency planning in support of aligned CCs.

As the CC is preparing for crisis execution, the GC is mirroring its activities. Figure 4 shows the parallel actions in the theater as the crisis unfolds. The JTF anchor in the GC C2 Center provides the JTF with continuous access to the networks, systems, and assessments that the GC has been working on during steady-state operations. The geographic anchor will also leverage personal relationships with the governments and involved organizations. This more radical approach to global engagement will have to be fleshed out to include specific manning with a focus on having a smaller net staff since JTFs will leverage multiple Service staffs. Personnel will be identified and trained for crisis response staffing and ready for mobilization and deployment.

FCCs will maintain the same mission areas, tasks, and funding lines. FCC C2 Centers will mimic the CC C2 Center's strategy, planning, and operations supported by an intelligence fusion center. Key to interaction with the GCs and CCs will be assigned LNO teams that will be imbedded across the CC and GC C2 Centers. These LNO teams will provide real-time connectivity to the functional experts and provide information on GC and CC requirements. The LNOs assigned to the GCs will contribute to the development of AOR-specific data on networks.

What Is Fixed and Not Fixed

This proposal represents a significant shift from the numbered, stovepiped staff structure and seeks to optimize changes in telecommunications and information systems technology. The two distinct missions of theater engagement and warfighting are separated, allowing the assigned staffs to focus on their mission without confusion or contradiction. There is also a clear path to establishment of a JTF in response to a crisis, with a defined network of support and links to existing organizations across the government. Resource competition is negotiated between the combatant commander and the other four-stars of the Joint Staff and the FCs without having to default to the Secretary or President.

If this option of restructuring commands without a J-staff is adopted, it must be done so across all commands in order to be effective and not repeat past mistakes. Should the Joint Staff abandon the classic staff structure? This is a discussion for another time, but the structure of the C2 relationships between the Secretary of Defense and the GCs and CCs will certainly change.

This proposal also relies heavily on an assumption of C2 connectivity. While modern forms of information technology provide great leverage in the battlespace, they come with their own costs and vulnerabilities. The effects of graceful, versus catastrophic, degradation of systems will be part of the pre-implementation assessment of this option. If the JTF staff loses connectivity or experiences a slowing of the information streams it is relying on, it must continue to execute the assigned mission with available resources. This is especially relevant at the tactical level, as units may find themselves cut off from higher headquarters.

Challenges will arise when a natural or man-made disaster escalates into a warfighting conflict. In assessing this proposal, General James T. Hill, USA (Ret.), was not in favor.[17] In his words:

Bottom line: [I] *do not like the idea of separating functions and staffs. Countries need one face and one voice to deal with. In my mind warfighting and nation-building/relationship-building* [are] *inseparable. My relationships allowed me to easily get*

countries to take up peacekeeping roles in Haiti [and] *allowed me to withdraw my warfighting forces and easily transition to Brazil peacekeepers. Only combatant commanders have the ability to do that.*

Finally, this approach will require a rigorous assessment of current U.S. Code, and what if any changes must be made to maintain legality. These changes will probably include examining the role of Service secretariats and the structure of Office of the Secretary of Defense.

Recommendation

In a time of funding demands for recapitalization, organizations look for increased efficiencies without decreasing overall effectiveness. Clear leadership roles, a focused staff, and an understanding of the operational environment are aspects of successful command and control relative to a CCMD. The missions of TSC and planning and execution remain incumbent on the structure of the U.S. military at some theater/nation-state level, if the current vision of maintaining a force that can be leveraged to address global conflict and natural and man-made disasters is to be maintained.

The Secretary of Defense and Chairman should consider implementing this proposal across DOD since it has the potential to increase efficiency by simplifying C2 organizations and focusing on critical areas relevant to understanding the battlespace and preparing for a crisis response. Added bonuses include a decrease in the number of four-star billets while maintaining a specific focus on theater engagement for the GCs.

Napoleon I died in 1821, having fought his last campaign at Waterloo in 1815, yet the staff structure built on his legacy lives on. After nearly 200 years, modern U.S. warfighting has evolved a standardized J-staff structure as well as modifications for Service components and coordination that reflect global engagement. Due to the stress of fiscal constraints with no commensurate decrease in tasking, DOD has an opportunity to either streamline existing theater command structures or establish a new paradigm for theater engagement to include TSC and warfighting. Changes will not be implemented without challenge by special interest groups and may require a fundamental change to the public laws of 10 U.S. Code to reflect new structures. Not adopting a significant change to the theater system will continue the existing status quo with a lack of coherence as the CCMDRs attempt to address all the concerns of the U.S. military in an increasingly complex world—in short, the continuance of ad hoc response to crises. The opportunity, indeed the requirement for change, is now. **JFQ**

Notes

[1] "Secretary of Defense Speech, Reagan National Defense Forum Keynote, as Delivered by Secretary of Defense Chuck Hagel, Ronald Reagan Presidential Library, Simi Valley, CA, November 15, 2014," available at <https://dod.defense.gov/News/Speeches/Speech-View/Article/606635/>.

[2] "Remarks by Secretary Carter in a 'Fireside Chat' at the United States Military Academy, West Point, New York," March 23, 2016, available at <https://dod.defense.gov/News/Transcripts/Transcript-View/Article/703031/remarks-by-secretary-carter-in-a-fireside-chat-at-the-united-states-military-ac/>.

[3] Jim Garamone, "Mattis Asks Congress for Stable Budgets, End to Sequestration," DOD News, June 12, 2017, available at <www.defense.gov/News/Article/Article/1211661/mattis-asks-congress-for-stable-budgets-end-to-sequestration/>.

[4] Edward J. Drea et al., *History of the Unified Command Plan, 1946–2012* (Washington, DC: Joint History Office, 2013).

[5] Adam Mazmanian, "Trump Elevates CyberCom to Combatant Command Status," *FCW.com*, August 18, 2017, available at <https://fcw.com/articles/2017/08/18/cybercom-elevated-to-unified-command.aspx>.

[6] The total number of Servicemembers in 1945 was 12,209,238. See "Research Starters: U.S. Military by the Numbers," The National World War II Museum, New Orleans, LA, available at <www.nationalww2museum.org/students-teachers/student-resources/research-starters/research-starters-us-military-numbers>. The total number of Servicemembers in 2017 was 2,875,500. See "Military Personnel," *GlobalSecurity.org*, available at <www.globalsecurity.org/military/agency/end-strength.htm>. The total U.S. population in 1940 was 132,165,129; in 1950, 151,325,798; estimated in 2018 at 327,421,076. See "Selected Historical Decennial Census Population and Housing Counts," available at <www.census.gov/population/www/censusdata/hiscendata.html>. The percentage of the population in the military in 1945 was 8 percent and 0.8 percent in 2017.

[7] Feickert, 2013, 14.

[8] Joint Publication 5-0, *Joint Operations Planning* (Washington, DC: The Joint Staff, June 16, 2017).

[9] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 3.

[10] Clark A. Murdock, *Beyond Goldwater-Nichols: Defense Reform for a New Strategic Era* (Washington, DC: Center for Strategic and International Studies, 2004), 75–77.

[11] John Grady, "Panel Advocates Reducing Number of U.S. Combatant Commands, Staff Size," USNI News, November 5, 2015, available at available at <http://news.usni.org/2015/11/05/panel-advocates-shirking-number-of-u-s-combatant-commands-staff-sizee>.

[12] Charles D. Sycora, "Has the Time Come to Merge SOUTHCOM with Another Unified Command?" (Master's thesis, U.S. Naval War College, 2004).

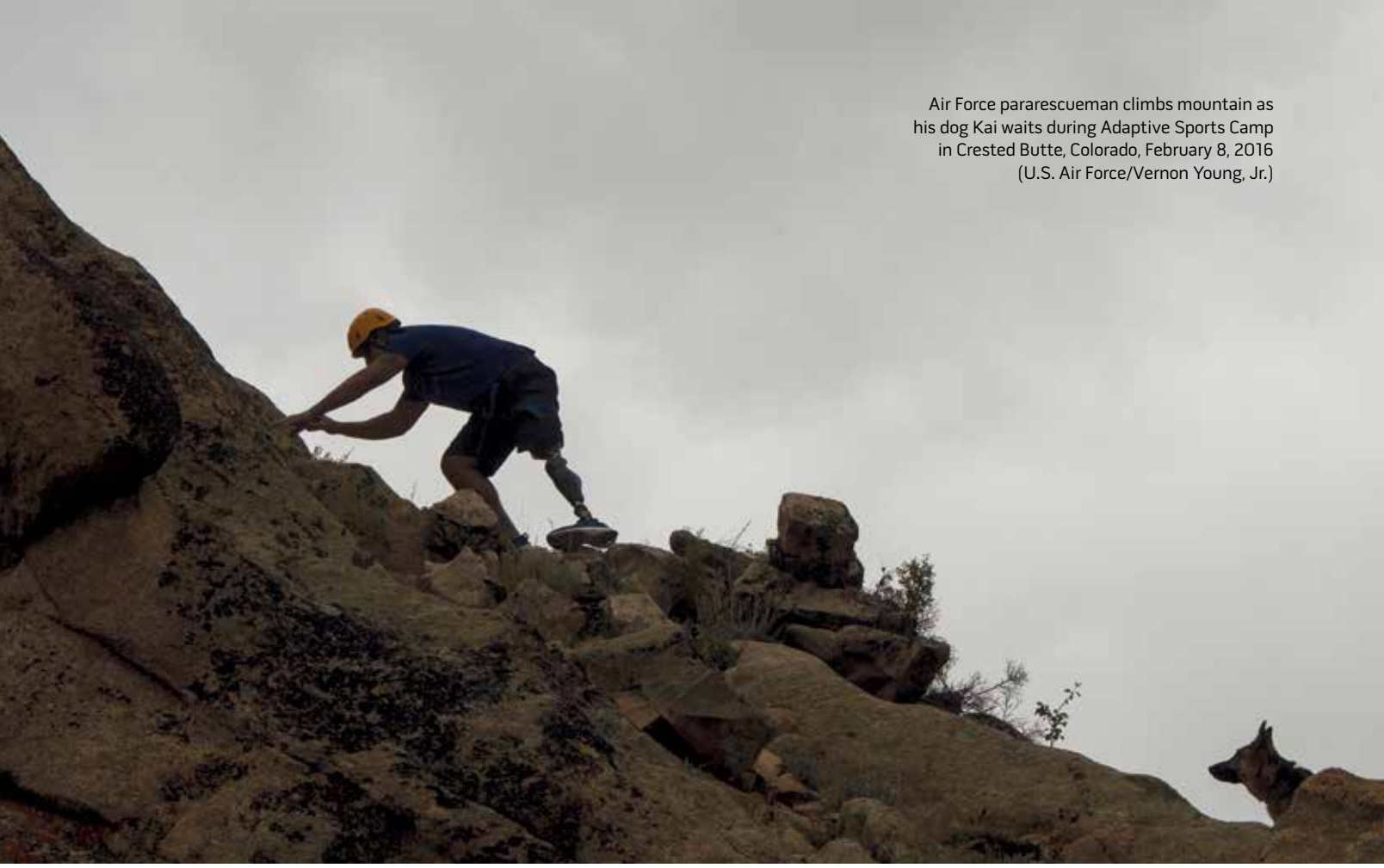
[13] Rhude Cherry III, "Reorganizing Geographic Combatant Command Headquarters for Joint Force 2020" (Master's thesis, Joint Forces Staff College, 2013).

[14] *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 8–12; *Summary of the 2018 National Defense Strategy of the United States of America*, 4.

[15] The author's color codes are Red, enemy; Blue, declared friends and allies who may be covered by treaty agreement; White, declared neutral; Gray, nationless states and stateless nations; and Green, friends who may provide indirect support to the enemy.

[16] David H. Ucko, "When Intervention Works: The Instructive Case of Sierra Leone," War on the Rocks, August 31, 2016, available at <https://warontherocks.com/2016/08/when-intervention-works-the-instructive-case-of-sierra-leone/>.

[17] Email from General James T. Hill to author, May 9, 2018.



Air Force pararescueman climbs mountain as his dog Kai waits during Adaptive Sports Camp in Crested Butte, Colorado, February 8, 2016 (U.S. Air Force/Vernon Young, Jr.)

Force Protection from Moral Injury

Three Objectives for Military Leaders

By Jeffrey Zust and Stephen Krauss

War makes us killers. We must confront this horror directly if we're honest about the true costs of war. . . . I'm no longer the "good" person I once thought I was. There's nothing that can change that; it's impossible to forget what happened, and the only people who can forgive me are dead.[1]

Chaplain (Colonel) Jeffrey Zust, MDiv, MAT, Mth, MS, is the First U.S. Army Command Chaplain. Captain Stephen Krauss, USA, Ph.D., is an Assistant Professor in the Consortium for Health and Military Performance at the Uniformed Services University of the Health Sciences.

Moral injury is an invisible wound that disrupts a Servicemembers' character, leaving them feeling "sad, mad, had, and/or bad." Specifically, moral injury is a complex "soul" wound caused by Servicemembers judging that their actions, or inactions, are contrary to their core values.[2] We cannot see the internal core of a person's being, but his narratives reveal the hidden contradictions that wound him. Research shows that the resulting effects from these hidden wounds are separable from post-traumatic stress

disorder (PTSD) and extend beyond the battlefield into units, families, and communities.[3] Servicemembers inherently make value-based, life and death decisions in the performance of their duties. These decisions are, in effect, moral decisions, and the contradictions within these decisions form a moral dissonance that alters the way Servicemembers view their existence. Thus, moral injury becomes a force protection threat that senior leaders can mitigate by preparing Servicemembers psychologically, socially, and spiritually for the moral risks and realities they will encounter in combat; embedding moral reasoning within mission command processes to provide clear moral "red lines" that guide professional practice; and building healing processes into postcombat actions that help Servicemembers address perceived moral contradictions.

Background

Leaders can influence, but not control, how Servicemembers will morally perceive traumatic events, either cognitively or emotionally. Veterans frequently take responsibility for even unintended contradictions of their core values and can react with guilt or anger to circumstances that they could not have influenced. Consider the example of a wounded squad leader who continually blames himself for failing to rescue his Soldier trapped in a burning vehicle. The squad leader had reservations about the chosen route for the mission, but he followed the order that led to the Soldier's death. He believes he should have done more as a "good" leader and feels guilty for breaking his promise to bring his total team home alive. His situation is just one of the cruel realities of combat. His perceptions may or may not be accurate, but they are his new reality. How will he recover? Can he find new meaning that helps him recover his sense of self, without denying the reality of what he experienced?

Leaders can aid their subordinates in this process by setting the conditions for how subordinates act, interpret, and process combat experiences.[4] The moral effects of combat can be severe. As one Air Force drone operator reflects, "I felt like I was haunted by a legion of the dead. My physical health was gone, and my mental health was crumbled. I was in so much pain, I was ready to eat a bullet myself."[5] A senior officer summarizes his service, "It is clear to me today that I, and others, sometimes failed to make wise choices. To our shame, we should have known better."[6] Leaders can mitigate the sources for these severe effects by incorporating moral reasoning into training, operating, and healing.

We are apt to focus more on the physical and psychological effects from traumatic events rather than the moral contradictions that contribute to moral injury. Moral injuries are not fear-based reactions to traumatic stress.[7] For example, one drone operator successfully killed a terrorist facilitator while sparing his child. He then watched through the screen as the child picked up the pieces of his father and, to his utter horror, placed them back into human shape.[8]

Evidence suggests that moral dissonance from unresolved contradictions between core values and perceptions of their experiences cause moral injury.[9] Moral dissonance is a normal response to perceived failure to live up to core values. It is experienced as a range of emotions such as doubt, anger, betrayal, regret, embitterment, shame, or guilt. High levels of prolonged moral dissonance build into moral injury.

Prepare Servicemembers for Moral Risks

The majority of Servicemembers exposed to the harshest realities of combat are also the youngest and least experienced. It is therefore imperative that junior officers and enlisted troops receive training that prepares them to respond morally as well as kinetically in combat. But research on moral decisionmaking does not fully support how morality is traditionally taught.

Research suggests that instead of formal moral systems guiding intuitive, gut-level responses to moral issues, people tend to use formal moral systems simply to justify their intuitive responses.[10] These responses develop similarly to how we developed our tastes for food or clothing—through life experience, not classroom instruction. Thus, George Washington was correct when he stated that when we took our oaths and donned our uniforms, we did not lay aside our sense of right and wrong.[11]

Servicemembers use their moral intuitions in both training and combat. They will do this regardless of whether abstract moral systems are addressed in our training doctrine, curriculum, and schedules. Therefore, if we want to help warfighters develop resiliency to combat stress, we need to help them develop the gut-level moral reasoning they will need to discern among the shades of gray they will encounter in war. This can be done through more fully integrating moral issues into skills training.

Leaders at all levels are in unique positions to develop moral reasoning within their subordinates, beginning with the incorporation of moral reasoning into the training of combat skills. Consider the following example of a commander introducing moral reasoning into a platoon live-fire range. During a movement to contact, his Soldiers intentionally killed a jackrabbit that hopped onto the objective. Technically, the Soldiers successfully completed their mission by taking the objective and shooting the designated "enemy" targets without firing upon the "civilian" targets. However, the commander took the lesson a step further. After completing the technical portion of the after-action review, the commander used the targeting of a "noncombatant" rabbit as a teaching moment to connect his unit's moral reasoning with their actions. He literally had his junior leaders and Soldiers walk through their reasoning as to why they were unable to refrain from killing a live, unarmed creature that posed no threat, under conditions where they were not in danger. In doing so, he directed them to consider their future targeting decisions and hopefully mitigated future behaviors that could morally harm his Soldiers.[12]

Combat is filled with complex events that warfighters may judge as contrary

to their core values. For example, one intelligence operative called in an airstrike on a house that had sustained gunfire coming out of a single window. He later found nine women and eight children among the dead. He relives seeing those 17 bodies almost daily.

Unresolved moral dissonance formed from moral judgments causes moral injuries. These unresolved moral contradictions are painful reminders that fuel negative judgments of personal character and military service.[13] Roughly 18.6 percent of combat veterans experience symptoms of PTSD.[14] However, a growing number of veterans who do not qualify for this psychiatric diagnosis still report ongoing suffering related to their moral judgments of their service.[15]

Not all Servicemembers experience harmful levels of moral dissonance from combat.[16] Research suggests that alignment of our values with our behavior helps protect combatants against a wide range of negative outcomes such as moral injury, PTSD, depression, and suicide.[17] In addition, we send units, not individuals, to war. Research suggests that cohesive units, and units with high morale, have lower levels of behavioral health problems regardless of amount of combat exposure.[18] Both cohesion and morale are formed within the social bonds that units develop during training. These bonds include the core values of the individuals forming them, mitigating the conditions that create moral injuries. In short, unit cohesion and morale protect Servicemembers from moral injury.

Leaders at all levels can shape training to help Servicemembers sharpen the moral reasoning that supports the standards they will practice in combat. During training, leaders also build the cohesive unit relationships that support how individuals resolve the harmful moral dissonance they may experience. However, these benefits can be destroyed by how units operate in combat.

Embed Moral Reasoning

After years of counseling morally wounded veterans, Department of Veterans Affairs' psychiatrist Jonathon Shay identifies failed leadership as one of the primary causes of moral injury.[19] When Soldiers burned a library as a reprisal during the Philippine insurrection, a young lieutenant named George C. Marshall told a fellow officer, "Once an army is involved in war, there is a beast in every fighting man which begins tugging at its chains. And a good officer must learn early on how to keep the beast under control, both in his men and himself."[20] This quotation has often been used to convey the moral responsibility that leaders possess in order to control how their orders influence behavior. Thus, controlling the beast within is a matter of describing how moral reasoning affects mission standards.

The exercise of moral reasoning goes deeper than setting a positive command climate. Sociologist Stjepan Mestrovic, a specialist in war crimes, believes that we can predict deviant, even criminal behaviors in combat units by the presence of dysfunctional command leadership. Fixing the blame for moral failures on rogue or bad actors often does not fix the larger picture of what really happens when combatants violate moral standards.[21] The effects of poor leadership spread throughout units.

In 2010, Soldiers from a Stryker platoon serving in Afghanistan were accused of intentionally killing an unarmed mullah. The prosecution focused on the leadership of a staff sergeant who had a "recruiting poster" military bearing and "sinister" motivations. However, the command investigation also described the greater effects caused by failed mission command that allowed the killing to happen. The investigator, Brigadier General Stephen Twitty, focused on the moral difference between a command *causing* criminal behavior and failing to *prevent* it. He wrote, "While the alleged criminal acts may have been identified earlier or perhaps prevented with stronger leader presence, I found nothing to indicate that the alleged criminal acts occurred as a result of the command climate set by the leaders above them. . . . At the same time, under different leadership, the crimes might never have happened."[22]

Not all moral failures are criminal. Research suggests that combatants will hold themselves accountable for group and personal events they failed to prevent or change.[23] They will also accept responsibility for their association with events in which they did not directly participate. This personal moral judgment leaves Servicemembers questioning their worth.[24] Resiliency against these types of moral injuries requires a mission command that links critical thinking and moral reasoning skills with operational practices.[25]

In the early phases of Operation *Iraqi Freedom*, a Marine platoon received orders prior to its mission that stated all personnel on the objective were considered hostile. Consequentially, the Marines wounded two unarmed shepherd boys. After the fight, the platoon leader regretted not clarifying what he believed to be an immoral order. He also believed that his orders contributed to his Marines' actions as an unintended consequence within the rules of engagement. However, he also knew that he and his Marines were reconciling their actions against a higher standard. Therefore, after the boys were treated and evacuated, he told his platoon: "Fellas, today was f____d up, completely insane. But we can't control the missions we get, only how we execute them. . . . I failed you this morning by allowing that 'declared hostile' call to stand. My failure put you in an impossible position."[26]

Later, when asked to explain his reasoning, he responded, "I tried to draw out those lessons for the platoon. First, we made a mistake this morning. . . . We don't shoot kids. When we do, we acknowledge the tragedy and learn from it."[27] Through a simple battlefield after-action review, this platoon leader hoped to shape his Marines' perceptions of the event by acknowledging their values, accepting responsibility for the past, and correcting a problem to shape future actions. Research suggests this type of transparent reasoning may help Servicemembers make sense out of their experiences, resolve their moral dissonance, and focus on their future in a healthy manner. This reformation of combat narratives helps reduce damaging effects from the moral dissonance formed during traumatic events.[28]

When commanders encourage combatants to "engage their brains before engaging their weapons," they are mitigating the potential for moral injury by linking their core values with target acquisition, a key warrior competency.[29] However, it does not necessarily establish the moral red lines combatants need to control their conduct in combat. Leaders often instruct subordinates to follow their moral compass without understanding that moral reasoning typically relies on gut-level intuitions that functions like a Global Positioning System to provide instant orientation without complex calculations.

Moral intuitions are influenced by repeated exposure, which is a process called habituation. In other words, moral intuitions are changed through repeated exposures to others' actions and by repeated commission of behaviors (both good and bad). In commands where "getting the job done" is the most important thing, this habituation can mean that immoral acts may no longer even be viewed as moral decisions. This is called moral fading. A recent U.S. Army War College report stated that moral fading is the result of a desensitization that "allows what should be an ethical decision to fade into just another way the Army does business."[30] As one captain proudly reported, to maintain a platoon leader on the battlefield, "I falsified the [traumatic brain injury] report that changed a distance from the [improvised explosive device] strike [to where] one person was standing."[31] What would happen if this platoon leader subsequently had issues from the brain trauma? Will this sort of moral event habituate the command toward more violations of Army values, further endangering trust in mission command?

Leaders can combat moral fading by focusing on moral reasoning that aligns mission orders, command intent, situational awareness, and good character. This type of mission command establishes red lines that contribute to mission success and guard combatants' character. Conversely, moral fading and misalignments within mission command degrade the essential links between core values and behavior that mitigate moral dissonance. Imagine the fading and misalignments that led the following decorated Ranger to describe his reasons for leaving military service: "The only two times where I personally was in a position to see where the Army had the choice to do the right thing or the wrong thing, both times they chose to do the wrong thing. . . . It made me realize that the Army does what suits the Army. That's why I won't put that uniform back on. I'm done."[32]

Grief-stricken American Infantryman whose buddy was killed in action is comforted by another Soldier, August 28, 1950, Haktong-ni area, Korea (U.S. Army/Al Chang)

This Ranger was personally involved in the events surrounding the death of Corporal Pat Tillman, and he experienced subsequent moral effects from how the military dealt with his unit, Tillman's family, and the American public *after* Tillman's death by friendly fire. Notice how his complaint is not based on traumatic affects from combat. Instead his complaint is focused on what he believes to be to be a failure within mission command based on what he perceives as a violation of both his and the Army's core values.

Each decision establishes some type of red line that controls the beast in every warfighter and forms some type of green light that permits warfighters to act. The very nature of the military profession is to win. In doing so, we fight in complex environments where combatants operate in situations that can easily lead to moral fading, blurring the moral red lines that guard their characters and identities.[33] Inevitably, misalignments and moral fading within mission command increase the likelihood that combatants ignore moral red lines in order to obtain a competitive advantage.[34] When this happens, moral injury becomes the likely consequence, as combatants' unresolved moral dissonance injures them, their units, their families, and their communities.

However, moral injuries are not the inevitable consequence of combat. Good military leadership incorporates moral reasoning within all phases of training and mission command. Incorporating moral reasoning into training and operations helps build resiliency and provide protections that mitigate the formation of moral injuries. Leaders at all levels can also facilitate recovery and healing processes, but postcombat resolution of moral dissonance is not a substitute for developing sound moral judgment during training and exercising it within mission command.

Remotely piloted aircraft qualification instructor pilot (left) conducts debrief of training mission with enlisted RPA student at 558th Flying Training Squadron, Joint Base San Antonio, Texas, July 17, 2018 (U.S. Air Force/Bennie J. Davis III)

Building Healing Processes

Combat produces moral dilemmas, and resolving the resulting dissonance is an essential part of the healing process. If Servicemembers can create positive meaning from their hardships, they may struggle, but they can avoid most, if not all, of the long-term behavioral health consequences associated with moral injuries.[35] The existence of moral dissonance implies the presence of a healthy conscience wrestling with the inevitable conflicts between core values and perceptions that occur during combat.[36] The resulting moral dissonance only develops into an injury if Servicemembers cannot successfully resolve this conflict.

Human beings have an innate need to understand, interpret, and judge traumatic events through iterative meaning-making processes in order to heal.[37] These cognitive and emotional healing processes begin spontaneously during traumatic experiences. The critical question is whether these processes help Servicemembers form an adaptive or maladaptive meaning for their lives.[38] This is likely why Air Force squadrons with social gathering places, called Heritage Rooms, have improved behavioral health outcomes over squadrons without such gathering places.[39] The same may be true for every unit that takes pride in its heritage. Good battle buddies or wingmen not only increase unit cohesiveness, but also aid in developing and maintaining a command climate that helps individuals resolve their moral dissonance and traumatic stress.

Direct access to professional help is essential in both deployed and garrison environments. Therefore, leaders must encourage their subordinates to get the help they need and work to dispel stigmas that prevent seeking professional help. Research is currently examining promising treatments for moral injuries involving cognitive and narrative therapies to help combat veterans harmonize their moral dissonance by assimilating and accommodating new meaning.[40] This harmonization results in a renewed sense of purpose for living. These types of therapies accomplish healing by focusing on adaptive practices that use core values to address damaging combat perceptions.[41]

Military leaders shape the future for defining and treating moral injury. Currently, moral injury does not have a universally accepted definition and to date, no research project has connected all the dynamics that happen when combat veterans experience harmful levels of moral dissonance. The most systematic and comprehensive look at the effects of combat stress on veterans from current operations derives from the Mental Health Advisory Team (MHAT). The MHAT collected data from Soldiers and Marines in nine studies conducted between 2003 and 2013. The surveys found that combatants reported negative perceptions of specific events that occurred during their deployments. However, the MHAT surveys did not ask Soldiers and Marines about the standards and core values they used in judging their perceptions or how their judgments affected their present behaviors and identities.

Leaders can help prevent moral injury and set the conditions for healing. The first step is to equip subordinates with the training and good moral leadership needed to mitigate and resolve their moral dissonance. The second step is to provide systemic resources to help identify, understand, and address moral concerns from training to battlefield and back home. This resourcing could range from conducting unit visitations and providing solid rules of engagement at the tactical level and providing embedded healers such as chaplains and combat stress teams at the operational level to establishing ongoing research and force protection policy at the strategic level. The objective is to create a military that integrates moral reasoning with mission command and healing practices that help warfighters serve honorably and return home ready for the future.[42]

Moral injury is a complex force protection issue that involves how warfighters prepare and return from combat. All combatants are moral actors because they make life and death decisions influenced by their core values and lethal skills. Leaders need to understand how combatants develop and use core values to judge perceptions of their military service and how unresolved moral dissonance from these judgments leads to maladaptive emotions, thoughts, and behaviors that become moral injuries.

Leaders can mitigate the risk for moral injury by establishing realistic training that prepares Servicemembers for the moral dilemmas they will encounter in combat,

embedding moral reasoning processes within mission command to establish clear boundaries for how combatants will operate, and providing healing resources to help them adopt adaptive practices to resolve their moral dissonance. Today's leaders cannot control all of the traumatic effects from combat, but they do set the conditions for moral reasoning, mission command, and the healing process that ensure our forces are ready for tomorrow's missions. **JFQ**

Notes

[1] Timothy Kudo, "I Killed People in Afghanistan. Was I Right or Wrong?" *Washington Post*, January 25, 2013.

[2] Duane Larson and Jeff Zust, *Care for the Sorrowing Soul* (Eugene, OR: Cascade Books, 2017).

[3] Joseph M. Currier, Jason M. Holland, and Jesse Malott, "Moral Injury, Meaning Making, and Mental Health in Returning Veterans," *Journal of Clinical Psychology* 71, no. 3 (2015), 229–240; Brett T. Litz et al., "Moral Injury and Moral Repair in War Veterans: A Preliminary Model and Intervention Strategy," *Clinical Psychology Review* 29, no. 8 (2009), 695–706; William P. Nash et al., "Psychometric Evaluation of the Moral Injury Events Scale," *Military Medicine* 178, no. 6 (2013), 646–652; Crystal L. Park, "Making Sense of the Meaning Literature: An Integrative Review of Meaning Making and Its Effects on Adjustment to Stressful Life Events," *Psychological Bulletin* 136, no. 2 (2010), 257.

[4] Timothy J. Hodgson and Lindsay B. Carey, "Moral Injury and Definitional Clarity: Betrayal, Spirituality, and the Role of Chaplains," *Journal of Religion and Health* 56, no. 4 (2017), 1212–1228.

[5] Pratrap Chatterjee, "American Drone Operators Are Quitting in Record Numbers," *The Nation*, March 5, 2015.

[6] Douglas A. Pryer, "Moral Injury: What Leaders Don't Mention When They Talk of War," Association of the United States Army, August 14, 2014.

[7] Currier, Holland, and Malott, "Moral Injury, Meaning Making, and Mental Health in Returning Veterans"; Litz, "Moral Injury and Moral Repair in War Veterans"; Nash, "Psychometric Evaluation of the Moral Injury Events Scale."

[8] Eyal Press, "The Wounds of the Drone Warrior," *New York Times*, June 13, 2018.

[9] Larson and Zust, *Care for the Sorrowing Soul*.

[10] Jonathan Haidt, *The Righteous Mind: Why Good People Are Divided by Politics and Religion* (New York: Vintage, 2012).

[11] George Washington, "Letter to the New York Provincial Congress, 26 June 1775," in *The Writings of George Washington from the Original Manuscript Sources, 1745–1799*, vol. 6., ed. John Clement Fitzpatrick and David Maydole Matteson (Washington, DC: Government Printing Office, 1931).

[12] Witnessed by Chaplain Zust during his Operation *Iraqi Freedom* tour with the 2nd Stryker Brigade Combat Team, 2nd Infantry Division, 2006–2008.

[13] Jacob K. Farnsworth et al., "The Role of Moral Emotions in Military Trauma: Implications for the Study and Treatment of Moral Injury," *Review of General Psychology* 18, no. 4 (2014), 249; Ronnie Janoff-Bulman, *Shattered Assumptions: Towards a New Psychology of Trauma* (New York: Simon and Schuster, 2010).

[14] Charles W. Hoge et al., "Combat Duty in Iraq and Afghanistan, Mental Health Problems, and Barriers to Care," *New England Journal of Medicine* 351, no. 1 (2004), 13–22.

[15] Terri Tanielian, *Assessing Combat Exposure and Post-Traumatic Stress Disorders in Troops and Estimating the Costs to Society*, Testimony Before the House Veterans' Affairs Committee, Subcommittee on Disability Assistance and Memorial Affairs, March 24, 2009, available at <www.rand.org/content/dam/rand/pubs/testimonies/2009/RAND_CT321.pdf>.

[16] Currier, Holland, and Malott, "Moral Injury, Meaning Making, and Mental Health in Returning Veterans."

[17] Crystal L. Park et al., *Trauma, Meaning, and Spirituality: Translating Research into Clinical Practice* (Washington, DC: American Psychological Association, 2017); Craig J. Bryan et al., "Meaning in Life, Emotional Distress, Suicidal Ideation, and Life Functioning in an Active Duty Military Sample," *The Journal of Positive Psychology* 8, no. 5 (2013), 444–452; Currier, Holland, and Malott, "Moral Injury, Meaning Making, and Mental Health in Returning Veterans."

[18] Yinyin Zang et al., "The Impact of Social Support, Unit Cohesion, and Trait Resilience on PTSD in Treatment-Seeking Military Personnel with PTSD: The Role of Post-Traumatic Cognitions," *Journal of Psychiatric Research* 86 (2017), 18–25.

[19] Jonathan Shay, "Trust: Touchstone for a Practical Military Ethos," in *Spirit, Blood and Treasure: The American Cost of Battle in the 21st Century*, ed. Donald E. Vandergriff (New York: Presidio Press, 2001), 3–20; Jonathan Shay, *Achilles in Vietnam: Combat Trauma and the Undoing of Character* (New York: Simon and Schuster, 2010).

[20] H. Paul Jeffers and Alan Axelrod, *Marshall: Lessons in Leadership* (New York: St. Martin's Press, 2010).

[21] Lieutenant General Stephen Twitty, USA, quoted in Luke Mogleson, "A Beast in the Heart of Every Fighting Man," *New York Times*, April 27, 2011.

[22] Ibid.

[23] Currier, Holland, and Malott, "Moral Injury, Meaning Making, and Mental Health in Returning Veterans"; Litz, "Moral Injury and Moral Repair in War Veterans."

[24] Carrie Doehring, "Resilience as the Relational Ability to Spiritually Integrate Moral Stress," *Pastoral Psychology* 64, no. 5 (2015), 635–649.

[25] Dick Couch, *A Tactical Ethic: Moral Conduct in the Insurgent Battlespace* (Annapolis, MD: Naval Institute Press, 2013).

[26] Nathaniel Fick, *One Bullet Away: The Making of a Marine Officer* (New York: Houghton Mifflin, 2006).

[27] Ibid.

[28] Park et al., *Trauma, Meaning, and Spirituality*.

[29] This quotation is from the instructions Lieutenant General James Mattis issued to each of his Marines on March 19, 2003, prior to engaging Iraqi forces.

[30] Leonard Wong and Stephen J. Gerras, *Lying to Ourselves: Dishonesty in the Army Profession* (Carlisle Barracks, PA: U.S. Army War College Press, 2015).

[31] Ibid.

[32] Jon Krakauer, *Where Men Win Glory: The Odyssey of Pat Tillman* (Norwell, MA: Anchor, 2010).

[33] Currier, Holland, and Malott, "Moral Injury, Meaning Making, and Mental Health in Returning Veterans."

[34] Dean C. Ludwig and Clinton O. Longenecker, "The Bathsheba Syndrome: The Ethical Failure of Successful Leaders," *Journal of Business Ethics* 12, no. 4 (1993), 265–273; Wong and Gerras, *Lying to Ourselves*; Dennis R. Balch and Robert W. Armstrong, "Ethical Marginality: The Icarus Syndrome and Banality of Wrongdoing," *Journal of Business Ethics* 92, no. 2 (2010), 291–303.

[35] Currier, Holland, and Malott, "Moral Injury, Meaning Making, and Mental Health in Returning Veterans"; Park, "Making Sense of the Meaning Literature."

[36] Larson and Zust, *Care for the Sorrowing Soul*.

[37] Park, "Making Sense of the Meaning Literature," 257.

[38] Park et al., *Trauma, Meaning, and Spirituality*.

[39] Wayne Chappelle, "Applied Status Report," presentation to the Consortium for Health and Military Performance and Walter Reed Army Institute of Research Center for Military Psychiatry and Neuroscience Performance Psychology Summit, February 26, 2018.

[40] Litz, "Moral Injury and Moral Repair in War Veterans."

[41] Brett T. Litz et al., *Adaptive Disclosure: A New Testament for Military Trauma, Loss, Moral Injury* (New York: Guilford Press, 2016).

[42] Farnsworth et al., "The Role of Moral Emotions in Military Trauma," 249.

Marines with Weapons Company, Battalion Landing Team, 3rd Battalion, 5th Marines, fire Carl Gustav rocket system during exercise Talisman Saber 17, Queensland, Australia, July 21, 2017 (U.S. Marine Corps/Amy Phan)

Thinking Differently about the Business of War

By Neil Hollenbeck, Arnel P. David, and Benjamin Jensen

Woven through our professional military discourse are threads of two different schools of thought with colors that clash. One school sees continuity in war and argues for renewed emphasis on core warfighting competencies. The other sees change in war and argues for reevaluation of the merits of those same competencies. A similar debate plays out in business literature. In a fiercely competitive and constantly shifting business environment, is success about the willingness to change with the times or the ability to focus on the fundamentals?

According to the 2018 National Defense Strategy, we are entering an era of great power competition and rapid technological change.[1] In his May 2017 testimony to the Senate Armed Services Committee, Chief of Staff of the U.S. Army General Mark Milley warned of "a fundamental change in the character of warfare."[2] His comments were consistent with predictions reported in a 2015–2016 Army study projecting trends likely to influence the future warfighting environment.[3] Among its conclusions were that the future U.S. military may be dramatically challenged by a convergence of factors, including the proliferation of low-cost sensors, precision-strike technology, robotics, and information technologies

Lieutenant Colonel Neil Hollenbeck, USA, is a Strategic Studies Fellow assigned to the Army Futures Command. Lieutenant Colonel Arnel P. David, USA, is a Strategist currently serving in the British Army. Dr. Benjamin Jensen holds a dual appointment as an Associate Professor at Marine Corps University and Scholar-in-Residence at American University.

that change how people receive, manage, and use information.

But new technologies do not revolutionize war. New *warfighting models*—that is, ways of organizing and fighting with technology—do.[4] This is what makes military preparedness during periods of rapid technological change so difficult. Applying the new tools to the same business is not enough. To fully exploit the potential of the new tools, we must actually change how we do business—sometimes radically. The business equivalent of a change in the character of war is *market disruption*. For all the attention lavished on "disruptive technology," new technologies do not disrupt markets. New business models—ways of profitably delivering value to customers—do.

According to a 2015 IBM survey of 5,200 senior executives, business leaders are increasingly concerned about getting blindsided by market invasion from competitors with a disruptive business model—a sudden, fundamental change in the character of market competition that renders a firm's business model obsolete.[5] What would be the consequences of our getting blindsided by war with a competitor employing a disruptive *warfighting* model? What if a U.S. military with 5th-generation fighter planes and upgraded armored brigade combat teams is defeated by an adversary employing the Internet of Things and low cost, long-range drones to exploit military potential we never fully appreciated?

Strategy in any domain is about risk-reward calculations and tradeoff decisions; one may better understand the problems of one domain by seeing them alongside their counterparts from another. We describe how the business concept of competitive advantage applies in a military context. Then, using both military and business examples, we discuss how matching our warfighting model to the future operational environment entails two separate, strategic dilemmas. The first is how we choose to manage the inevitable mismatch between the requirements of the wars for which we optimize our force and those of the wars for which we do not—a dilemma we face in any technological future. The second is how we mitigate the risk of strategic surprise by an adversary who fights with new technologies in a way that directly challenges our core warfighting model. Finally, we argue that, counterintuitively, the best strategy for avoiding strategic surprise could be to postpone large investments in specific systems.

Competitive Advantage in Business and War

At the heart of business strategy is an idea that lends itself to the military context—the concept of competitive advantage. A firm exploits a competitive advantage by tailoring its business model to its strengths and weaknesses relative to those of competitors. Business strategy revolves around cost and differentiation.[6] One firm may use a low-cost structure to undersell competitors. Another may garner price premiums by delivering value that its competitors cannot. Many kinds of advantages—for example, access to material, production experience, intellectual property, distribution networks, and alliances—can enable competition on one basis or the other. Business schools teach future managers to focus on sources of *sustainable advantage*—assets or attributes that competitors cannot easily replicate or nullify.[7]

Between 1987 and 2002, for example, American automakers responded to global competitors by incrementally improving vehicle quality and adding new features. But foreign competitors copied them so quickly that American automakers gained no lasting advantage.[8] In contrast, by introducing new sport utility vehicles and minivans, a vehicle class that foreign automakers lacked the experience and infrastructure to produce, American automakers gained a leap-ahead advantage they sustained for much longer.[9]

A source of competitive advantage need not be material. A company like Google might regard its human capital and culture as a source of advantage.[10] The U.S. Army, which spent the Cold War preparing to fight a technological near-peer, looked to doctrine, leadership, and training as sources of competitive advantage.[11] This thinking was evidenced by General Norman Schwarzkopf's statement that the 1991 Gulf War would have been a lopsided victory for the United States even if the U.S. and Iraqi militaries had traded equipment.[12]

The U.S. military entered World War II with multiple deficiencies relative to the seasoned German armies then rampaging across Europe and North Africa. But the United States had advantages in geography, industry, and alliances. Around those advantages we employed a warfighting model suitable for the competitor and the competition. General Walter Smith characterized an aspect of it with his quip, "The American Army does not solve its problems, it overwhelms them."[13]

After 1945, facing a different competitor relative to which the U.S. military lacked some of those strengths, American strategists chose a different warfighting model built around different advantages.[14] To defend Europe from the Soviet Union's massive ground armies, the U.S. military positioned itself to compete on differentiation—fielding forces that could do things their Soviet competitors could not. Early on, America's lead in nuclear weapons nullified Soviet advantages in mass. When the Soviets closed that gap, the United States invested in smaller but qualitatively superior conventional forces, including skilled air forces equipped with stealth aircraft, precision-guided munitions, and well-equipped, aggressive ground forces trained to fight outnumbered and win.[15]

This warfighting model proved well-adapted to the requirements of the 1991 Gulf War. But in the words of Harvard Business School Professor Clayton Christensen, "The very processes and values that constitute an organization's capabilities in one context define its *dis*abilities in another."[16] Subsequent wars in Iraq and Afghanistan illustrated that a warfighting model optimized for war with a military peer—the military equivalent of an important but narrowly bounded area of business competition—could not transform resource inputs into security outputs with the same efficiency in a *counterinsurgency*—a competition

Personnel from Santa Fe Drilling Company and Red Adair Oil Well firefighters battle blaze from burning oil well set afire by Iraqi forces prior to their retreat from Kuwait during Operation *Desert Storm* (DOD/Dick Moreno)

that places only moderate value on attributes the U.S. military possesses in abundance and great value on ones it could not be reasonably expected to simultaneously display.

Facing the dilemma of a mismatch between their capabilities and the requirements of a particular competition, the U.S. military and businesses have used different versions of the same strategies.

The First Strategic Dilemma: Mismatch

Strategy One: Say No. In 1992, almost immediately following the U.S. military's spectacular Gulf War victory, the Chairman of the Joint Chiefs of Staff, General Colin Powell, strongly opposed a limited military intervention in Bosnia. The 1991 Gulf War, in which we used overwhelming force to defeat a Soviet-style infantry and tank army in open battle, had fit our military's warfighting model well. But General Powell warned Americans not to expect similar results with the same military in a fundamentally different mode of war. He stated, "As soon as they tell me 'surgical,' I head for the bunker."[17]

Ultimately, political leaders overruled General Powell, and the U.S. military acted in Bosnia with mixed results. Many seasoned business leaders could sympathize—one may disagree with the boss's strategy and still be charged with making it work. But they also understand that there are strategic considerations beyond how well a market competition matches a company's business model. For example, securing a position in a backwater market may prevent competitors from securing a foothold from which they could threaten a more important market.

Over the courses of their careers, business and military leaders should expect to tackle mismatches and to be judged, not unfairly, on the skill with which they handle them. Powell, for his part, oversaw multiple successful, niche market applications of U.S. military force. These included the removal of a dictator in Panama, a mission to rescue stranded international citizens in Liberia, and humanitarian relief operations in Bangladesh.[18]

Strategy Two: Be Yourself. "Hope is not a method" is a soldier's adage. It means that to address the problem merely by hoping against its worst outcomes is not to address the problem. But there are times when the strategy has appeal. In business, for example, adapting parts of a firm to improve performance in one market may weaken a firm's performance in another.

Professor Christensen wrote that a firm's resources, processes, and values determine what it can and cannot do. All three must align with the firm's business

model.[19] Its processes and values can make it successful in one market but not another, even if its resources are valuable in both.

Similarly, in the 1990s, custodians of the U.S. military's warfighting model resisted military missions they categorized as "operations other than war," such as peacekeeping.[20] President Bill Clinton's national security advisor summarized the view when he wrote, "Our armed forces' primary mission is not to conduct peace operations but to win wars. . . . We will never compromise military readiness to support peacekeeping."[21] Those who supported giving such missions to the military still resisted suggestions that the military be deliberately organized, trained, and equipped for them. They feared that, no matter what resources they retained, an organizational focus on peacekeeping and low-intensity conflicts might slowly distort the processes and values that made the U.S. military dominant in its most important conflict market—high-end, conventional war.[22]

These leaders understood that executing a strategy means making tradeoffs.[23] These are analogous to the phenomenon microbiologists call "fitness tradeoff," or "fitness cost."[24] When a microorganism adapts to become fitter in one environment, it often becomes less fit in another. For example, an organism that evolves to survive in cold environments may become less fit for warm environments. Business leaders taking the long view may rightly decide to reject a business model adaptation if the fitness cost in one market outweighs the fitness benefit in another. Military leaders, hedging against a myriad of future threats, do the same, but not always with satisfactory results.

During the 2000s, waging counterinsurgency with a military optimized for high-end war, the United States had excess capacity in assets it needed least, like heavy artillery and high-performance aircraft, and insufficient capacity from those it needed most, such as infantry, special operators, and civil affairs soldiers. Furthermore, military processes and values optimal for high-end war, designed to deliver shock and destruction, were often counterproductive in situations that required nuance and restraint. Facing the consequences of a severe model mismatch, the U.S. military embraced strategy three.[25]

Strategy Three: Adapt. The rationale for adapting a firm's business model to the needs of a market it serves is evident. In hard times, even massive firms with deeply rooted cultures, like General Electric (GE) and IBM, change.[26] So did the U.S. military during the Iraq War—an adaptation popularly associated with the 2007–2008 Surge campaign.[27] What happened in Iraq at that time and which factors most contributed remain hotly debated. But that the U.S. military adapted in response to a mismatch is not.

Today, U.S. military equipment, training, and culture—its resources, processes, and values—better position it for agility across a spectrum of mission types, from advising partners in the fight against the so-called Islamic State to full-scale war on the Korean Peninsula.[28] But while the generals of 2007 wrestled with the mismatch between the military's high-end warfighting model and a low-end conflict market, the generals of 2019 are taking inventory of the fitness tradeoffs made since 2001. As General Milley explained, "Today, a major in the Army knows nothing but fighting terrorists. . . . As we get into the higher end threats, our skills have atrophied over 15 years."[29] This begs the question, if it is hard for an organization good at many things to be good at anything, why not divide and specialize?

Strategy Four: Divide and Specialize. A common business response to a mismatch is to create a substantially separate business unit to optimize for the unique market. This is what Google did in 2015, when it created a parent company, Alphabet, so that leaders of different business units could "run things independently that aren't very related."[30] This is also what the U.S. Army did, in 1947, when it spun-off its air arm to create a separate military Service, the U.S. Air Force.

The first military aircraft in history was a Wright Model A, purchased by the Army in 1909. As aircraft technology matured, it played an increasingly significant role in war. Army aviation, consolidated into the Army Air Corps in 1926 and Army Air Force in 1941, grew increasingly focused on air operations not directly related to ground combat.[31]

In 1947, the United States created a parent organization, the Department of Defense (not so named until 1949), under which it organized the Departments of the Army, Navy, and newly independent Air Force.[32] The Marine Corps remained a separate military Service within the Department of the Navy—an organization optimized from its inception for a niche market within the wider market of maritime warfare. Today, some observers question whether cyber warfare might become such an important and unique market that it warrants its own military Service.[33]

In the 1960s, contemplating response options in the face of communist subversion in Asia, Latin America, and elsewhere, President John F. Kennedy believed that the U.S. warfighting model offered him only two choices: take no action or employ large conventional forces and risk war with the Soviet Union.[34] At the low end of war, he perceived an underserved market. Therefore, he championed investment in special operations forces.[35] Over time, Green Berets, optimizing for the unique markets they serve, have grown increasingly independent of and culturally distinct from the wider Army.

Divide and specialize strategies can be particularly attractive. But they can also have hidden costs. With the creation of separate air forces, the Army lost control of certain types of aircraft that support ground operations. In contrast, the Marine Corps maintains its own fleet of jet fighters, separate from those of the Air Force or Navy. In creating Special Forces, the Army also subjected its other units, especially ground combat units, to internal competition for talent.

The Second Strategic Dilemma: Disruption

Volumes of business literature address firms' failures to survive business model disruption. Business students study the demise of Kodak and Blockbuster

U.S. Special Forces conduct downed pilot simulation using new gear to assess operational effectiveness for Army Warfighting Assessment 17.1 exercise at Fort Bliss, Texas, October 18, 2016 (U.S. Army/Alexander Holmes)

the way West Point cadets study the defeat of the Spanish Armada in 1588 and of Poland and France in 1939 and 1940, respectively. The latter were historic military upsets in which victors combined one or more new technologies with innovative tactics, not only winning battles but also changing how such battles were fought.[36]

As the rate of technological change increases, so does business executive bandwidth devoted to horizon-scanning for threats and opportunities. The U.S. military and its adversaries are doing the same. But recognizing that technology will emerge is not the same as knowing which technologies will create what effects and how quickly.

In the business context, an *innovation* is simply a change in technology—any change in how inputs are transformed into outputs.[37] This applies to changes in organizational methods and processes as well as changes in machines, materials, software, and so forth. But a leap-ahead technology, even if rooted in a novel approach, need not be disruptive. To be disruptive, it must change the *basis* of market competition in ways not suited to the dominant business models. For example, the compact disc was a leap-ahead improvement over the cassette tape. No firm in the music recording industry could have retained its market position without transitioning. But it did not change the commonly recognized dimensions of the product value—capacity, portability, and sound quality. It was firms already dominant in the industry, Sony and Philips, that introduced the technology and they remained secure.[38]

When a market-disrupting threat appeared, it came from an innovation that delivered slightly *worse* sound quality—the MP3.[39] This made music so much more portable that new business models became possible.[40] Suddenly, a firm like Pandora could threaten the positions of firms established in the market for decades.

In protracted competition, an organization must evolve with the environment and respond quickly when the basis of competition changes. In their 2011 *HBR* article, "The CEO's Role in Business Model Reinvention," Vijay Govindarajan and Chris Trimble wrote that established firms rarely find "the next big thing" before new entrants, explaining "many companies become too focused on executing today's business model and forget that business models are perishable."[41]

But the challenge runs deeper. Even when firms can see change on the horizon, it is hard for an organization to maintain the edge in one game and

Installation of commercial Internet and phone packages at worldwide regional hub nodes, such as this one in Camp Roberts, California, enables Army and National Guard units to provide commercial services during emergency incidents anywhere on Earth (U.S. Army)

simultaneously position itself for another. When attributes that may or may not be valuable in the far term have limited utility in the near term, reasonable organizational processes constrain investment in them.[42]

This is why technologies that will eventually disrupt business markets are often not delivered by the firms already established within them.[43] In these cases, other firms introduce the technologies to different, sometimes niche, markets where their weaknesses matter less and their unique strengths matter more.[44] There, in the laboratory of real-world application, the technologies mature.[45] Once they reach performance thresholds necessary for them to be competitive in other market, they take the market by storm.[46] Development of U.S. naval aviation is as good an example as any from business.

In the 1920s, some theorists argued that aircraft could displace battleships in the market for destruction of enemy warships.[47] Aircraft of that era lacked the range, payload capacity, and mechanical reliability for this, but they found their way into a niche military application—aerial reconnaissance.[48] There and in civil applications the technology matured until it met performance thresholds that forced navies to redesign their warfighting models around not battleships, but aircraft carriers.[49]

The first strategic dilemma, mismatch, we can never escape; we can only manage it. But disruption is avoidable, and we do so by the following.

First, look for how new technology could enable new ways to win. Markets are not disrupted by new technology; they are disrupted by new business models. Henry Ford did not invent the automobile, the assembly line, or interchangeable parts.[50] His company offered a value proposition—rapid and reliable personal transport—at a price point it could achieve with the cost structure those technologies allowed.[51] To be fair, Ford did improve those technologies. But consider Uber, whose founders did not improve the Internet, the smart phone, or data analytics. They simply built a business model from them.

From 1939 to 1940, the German military stunned the world by forcing the rapid collapse of massive, modern militaries with methods journalists of the time dubbed *blitzkrieg* (Lightening War). Enabling blitzkrieg were the tank, airplane, and two-way radio.[52] But these were not new technologies. All had been in use for over 20 years and had seen heavy employment on both sides of World War I. The German army may not

have deliberately conceived of a new way of war so much as stumbled into one, as maturing technologies unlocked latent potential in its doctrine and organizational culture. But whatever its genesis, the game changer was the warfighting model that emerged, not the technology.

Second, do not go big where you should go small. In 1992, Hewlett-Packard (HP) made a large investment in developing a leap-ahead disk drive technology—the Kitty Hawk—for an emerging market.[53] Demand appeared just as HP predicted, but customers' specific requirements were not what it expected. By the time it was evident that the Kitty Hawk, as designed, was ill-suited to the market that was actually emerging, Kitty Hawk's managers had neither the resources nor the credibility to reengineer it. The program folded.

There are parallels in the Army's Future Combat Systems (FCS) experience. In the 1990s, the Army recognized that it was investing mostly in incremental improvements to current technologies. To drive a leap ahead, it focused on opportunities and threats 15 or more years in the future.[54] One outcome was the FCS program. Aimed at a distant future and seeded with layers of technical risk, the program struggled. By 2009, with shifting priorities and too little to show for its $18 billion investment, the Department of Defense canceled the system.[55]

Christensen argues that purveyors of new technologies must conserve resources to survive early market failures so they can deploy their resources when the right investment becomes evident.[56] This is the business equivalent of the military principle of making contact with the smallest element possible. That is, when entering an area within which the enemy disposition is unknown, the commander holds back large units and advances small ones to develop understanding through contact with the enemy.

For HP, this would have meant producing different, perhaps less expensive variations of the Kitty Hawk to test in different markets. For the Army, this may have meant smaller investments in a large number of lower cost programs with fewer interdependencies. One may recognize this as similar to a venture capital approach, but there is Cold War precedent for it.

In his book *Winning the Next War: Innovation and the Modern Military*, Harvard Professor Steven Rosen described how the U.S. military approached missile development from 1946 through the 1950s. Intercontinental bombardment was new and multiple means of it were conceivable.[57] The military could not know which would be most effective or what the Soviets would choose. Since missiles were expensive, the U.S. military hedged, deliberately making small investments in a portfolio of prototypes without fully fielding any.[58] In doing so, leaders were trading *early* capability for knowledge that would allow them to quickly create the *right* capability once it became evident, if not also to foresee it faster than the Soviets.

Finally, go big where you cannot go wrong. When allocating finite resources, investments that pay off in multiple futures are especially sound. For example, in 2011, GE decided to connect all of its manufacturing machines to an Industrial Internet of Things. GE reasoned that once it developed expertise in digital industrial manufacturing, it could build a business model around industrial analytic services.[59] The genius of GE's strategic decision was not in divining the future of the industry; it was investing in a capability that, coupled with its unique market position, would be a source of competitive advantage in almost any future. Investments in the application of technologies enabled by artificial intelligence to military problems may be an example.

Military strategy in protracted competition is, to a great degree, organizational strategy. We organize, train, and equip according to assumptions about what will matter most in future wars. It is good that we are examining and vigorously debating those assumptions. But guessing better than our adversaries is not enough because the winning long-term strategy may not be that which proceeds from the best assumptions. It may be that which most honestly acknowledges uncertainty about the future and then best accounts for it. **JFQ**

Notes

[1] *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 1.

[2] Mark A. Milley, quoted in *Stenographic Transcript Before the Committee on Armed Services, United States Senate: Posture of the Department of the Army* (Washington, DC: May 25, 2017), 31, available at <www.armed-services.senate.gov/imo/media/doc/17-54_05-25-17.pdf>.

[3] *The Character of Warfare 2030–2050: Technological Change, the International System, and the State*, U.S. Army study report (Washington, DC: Chief of Staff of the Army Strategic Studies Group, March 2016).

[4] The authors have deliberately avoided using a term such as *operating* or *operational concept*. These are warfighting models, but the terms have different meanings to different readers.

[5] IBM Institute for Business Value, *Redefining Boundaries: Insights from the Global C-Suite Study* (Somers, NY: IBM Global Business Services, 2015), 1, available at <https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03695usen/gbe03695-usen-03_GBE03695USEN.pdf>.

[6] Roger L. Martin, "There Are Still Only Two Ways to Compete," *Harvard Business Review* (April 21, 2015), available at <https://hbr.org/2015/04/there-are-still-only-two-ways-to-compete>.

[7] Jay Barney, "Firm Resources and Sustained Competitive Advantage," *Journal of Management* 17, no. 1 (1991), 99–120, available at <www.bms.lk/download/PGD/slides/Strategic-Planning-Materials/Barney-1991-strategy.pdf>.

[8] Martin Neil Baily et al., *Increasing Global Competition and Labor Productivity: Lessons from the U.S. Automotive Industry* (New York: McKinsey Global Institute, November 2005), 85–91.

[9] Ibid.

[10] Laszlo Bock, *Work Rules! Insights from Inside Google That Will Transform How You Live and Lead* (New York: Grand Central Publishing, 2015).

[11] Benjamin Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Palo Alto: Stanford University Press, 2016).

[12] Winslow Wheeler, "Not All That It Can Be," *Foreign Policy* (October 12, 2012), available at <https://foreignpolicy.com/2012/10/12/not-all-that-it-can-be/>.

[13] John Ellis, *Brute Force: Allied Strategy and Tactics in the Second World War* (New York: Penguin Books, 1990), 525.

[14] U.S. grand strategy after 1945 revolved around alliances and political warfare as much as military posture. However, only military

components of that grand strategy are within the scope of this article.

[15] R.Z. Alessi-Friedlander, "Learning to Win While Fighting Outnumbered: General Donn A. Starry and the Challenge of Institutional Leadership during a Period of Reform and Modernization," *Military Review* (April 26, 2017, online exclusive), available at <www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2017-Online-Exclusive-Articles/Learning-to-Win-While-Fighting-Outnumbered/>.

[16] Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Boston: Harvard Business Review Press, 1997), xxvii.

[17] Michael R. Gordon, "Powell Delivers a Resounding No on Using Limited Force in Bosnia," *New York Times*, September 28, 1992, available at <www.nytimes.com/1992/09/28/world/powell-delivers-a-resounding-no-on-using-limited-force-in-bosnia.html?pagewanted=all&mcubz=0>.

[18] Colin L. Powell, "U.S. Forces: Challenges Ahead," *Foreign Affairs* (September 10, 2017), available at <www.foreignaffairs.com/articles/1992-12-01/us-forces-challenges-ahead>.

[19] Christensen, *The Innovator's Dilemma*, 161–168.

[20] Joint Publication 3-07, *Joint Doctrine for Military Operations Other Than War* (Washington, DC: The Joint Staff, June 1995), vii.

[21] Anthony Lake, "The Limits of Peacekeeping," *New York Times*, February 6, 1994, available at <www.nytimes.com/1994/02/06/opinion/the-limits-of-peacekeeping.html?mcubz=1>.

[22] Dennis Rogers, "Maintaining a Constabulary Capability within the U.S. Military," U.S. Army War College research paper, 2001, 10–11.

[23] Michael E. Porter, "What Is Strategy?" *Harvard Business Review* (November–December 1996), available at <https://hbr.org/1996/11/what-is-strategy>.

[24] Dan I. Andersson and Diarmaid Hughes, "Antibiotic Resistance and Its Cost: Is It Possible to Reverse Resistance?" *Nature Reviews Microbiology* 8 (March 2010), 260–271, available at <www.nature.com/nrmicro/journal/v8/n4/full/nrmicro2319.html>.

[25] Nelson Granados, "The Sleeping Giant Awakes: Is Disney Too Late to Succeed in Streaming?" *Forbes* online, August 9, 2017, available at <www.forbes.com/sites/nelsongranados/2017/08/09/disney-to-stream-its-own-movies-without-netflix-will-it-succeed/#c5b056b4ef00>.

[26] Jeffrey Immelt, "How I Remade GE," *Harvard Business Review* (September–October 2017), available at <https://hbr.org/2017/09/inside-ges-transformation>; and Charles O'Reilly, J. Bruce Harreld, and Michael L. Tushman, "Organizational Ambidexterity: IBM and Emerging Business Opportunities," Rock Center for Corporate Governance Working Paper No. 53, Stanford Graduate School of Business, May 2009, available at <www.gsb.stanford.edu/faculty-research/working-papers/organizational-ambidexterity-ibm-emerging-business-opportunities>.

[27] Kimberly Kagan, *The Surge: A Military History* (New York: Encounter Books, 2009), 27–40.

[28] TRADOC Pamphlet 525-3-1, *Win in a Complex World* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2014), 22–24.

[29] Helene Cooper, "Long Emphasis on Terror May Hurt U.S. in Conventional War, Army Chief Says," *New York Times,* May 15, 2016, available at <www.nytimes.com/2016/05/16/world/africa/army-milley-africa-terrorism-land-war.html?mcubz=0>.

[30] Sam Sanders, "Google Creates a New Parent Company called Alphabet," National Public Radio, August 10, 2015, available at <www.npr.org/sections/thetwo-way/2015/08/10/431388769/google-creates-new-parent-company-called-alphabet>.

[31] Herman Wolk, "Toward Independence: The Emergence of the U.S. Air Force, 1945–1947," Air Force History and Museums Program, 1996, 1–4, available at <www.dtic.mil/dtic/tr/fulltext/u2/a433273.pdf>.

[32] "The National Security Act of 1947," Center for Security Policy, January 26, 2007, available at <www.centerforsecuritypolicy.org/2007/01/26/the-national-security-act-of-1947-2/>.

[33] Matthew Hyland, "Creating a New Military Service: Historical Precedents" (Master's thesis, School of Advanced Air and Space Studies, 2016), 72.

[34] Daniel C. Koprowski, "John F. Kennedy, the Development of Counterinsurgency Doctrine and American Intervention in Laos, 1961–1963" (Master's thesis, University of Massachusetts Amherst, 2014, available at <http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=2818&context=theses>.

[35] Mark Moyar, *Oppose Any Foe: The Rise of America's Special Operations Forces* (New York: Basic Books, 2017), 129–131.

[36] Paul Davis, *100 Decisive Battles from Ancient Times to the Present* (Oxford: Oxford University Press, 1999), 203, 376.

[37] Melissa Schilling, "What's Your Best Innovation Bet," *Harvard Business Review* (July–August 2017).

[38] Devon Shapiro et al., "The Invention of Compact Discs," Tuck School of Business at Dartmouth College, November 2012, available at <http://faculty.tuck.dartmouth.edu/images/uploads/faculty/ron-adner/dup-1EIS_Main_Project_Compact_Disc_Paper.pdf>.

[39] Ibid.

[40] Ibid.

[41] Vijay Govindarajan and Chris Trimble, "The CEO's Role in Business Model Reinvention," *Harvard Business Review* (January–February 2011), 109.

[42] Christensen, *The Innovator's Dilemma*, xxvii.

[43] Ibid., 24. Christensen's comments here are regarding the disk drive industry.

[44] Ibid., xix.

[45] Ibid., 54–55.

[46] Ibid., 72. Christensen's comments here are regarding the mechanical excavator industry.

[47] William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power* (Philadelphia: Curtis Publishing Company, 1925), 110.

[48] Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), 70.

[49] Ibid., 71.

[50] Ransom Olds, of Oldsmobile, introduced the assembly line to the automotive industry and patented the process in 1901. Interchangeable parts were invented by Honoré LeBlanc, an 18th-century French gunsmith, but were made popular by Eli Whitney's use of interchangeable parts in weapons he manufactured for the U.S. Government in the early 19th century.

[51] W. Chan Kim and Renee Mauborgne, "Blue Ocean Strategy," *Harvard Business Review* (October 2004).

[52] Allan R. Millett, "Patterns of Military Innovation," in *Military Innovation in the Interwar Period*, ed. Williamson Murray and Allan Millett (New York: Cambridge University Press, 1996), 339.

[53] Christensen, *The Innovator's Dilemma*, 146–149.

[54] Christopher G. Pernin et al., *Lessons from the Army's Future Combat Systems Program* (Santa Monica, CA: RAND, 2012), 7–10.

[55] Ibid., xvii–xviii.

[56] Ibid., 155.

[57] Ibid., 245–247.

[58] Ibid., 236.

[59] Immelt, "How I Remade GE."

President Nicolás Maduro of Venezuela and President Vladimir Putin discussed bilateral relations and measures to stabilize oil market, Beijing, September 3, 2015 (President of Russia Web site)

Evasive Maneuvers

How Malign Actors Leverage Cryptocurrency

By Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden

All the perplexities, confusion and distress in America arise, not from defects in their Constitution or Confederation, not from want of honor or virtue, so much as from the downright ignorance of the nature of coin, credit and circulation.

—John Adams, letter to Thomas Jefferson, August 25, 1787

Colonel Sara Dudley, USA, is assigned to Joint Special Operations Command. Lieutenant Colonel Travis Pond, USAF, is the Program Acquisition Evaluator at the Department of Defense Office of the Inspector General. Colonel Ryan Roseberry, USA, is an Intelligence Officer assigned to George C. Marshall Center. Colonel Shawn Carden, USA, is the Director of Future Operations at U.S. Army Cyber Command G35.

The U.S. National Defense Strategy outlines a fundamental competition between free and open societies and revisionist powers and rogue regimes. These powers and regimes frequently act below the threshold of war, enabled by recent technological advances. Effective responses to these advances demand creative solutions. The emergence of cryptocurrencies represents a novel frontier that diminishes U.S. comparative advantage in mapping funding to threat networks worldwide. By disrupting the visibility and control present within the traditional centralized international banking system, the use of cryptocurrencies negates the ability

for U.S. personnel to monitor and restrict funding sources. The ability to follow the money is at risk based on peer-to-peer exchange of encrypted currencies. To probe this vulnerability, explanations of blockchain technologies and cryptocurrencies show how adversaries use the technology to circumvent financial market control and sanction protocols. The U.S. Government will need to act to mitigate the current risk in poorly governed cryptocurrency market places.

Explaining Cryptocurrency

The global economic system has benefited substantially from the establishment of the free market system since the end of World War II. In 1944, the Bretton Woods Agreement established the U.S. dollar (USD) as the world's reserve currency, providing stability and liquidity that enabled significant growth in international trade. At that time, the USD was backed by U.S. gold reserves, which were the largest in the world.[1] In 1971, President Richard Nixon eliminated the exchangeability of USD for gold, but the strength of the U.S. economy and the norms of international trade created over the previous 20-plus years allowed the USD to retain its status as the world's reserve currency. The market confidence in the U.S. economy, along with centralized governmental monetary policy, continue to support the valuation of the USD internationally. Decentralized cryptocurrencies threaten to undermine the dominance of the USD due to the ways in which they can subvert the global financial system.

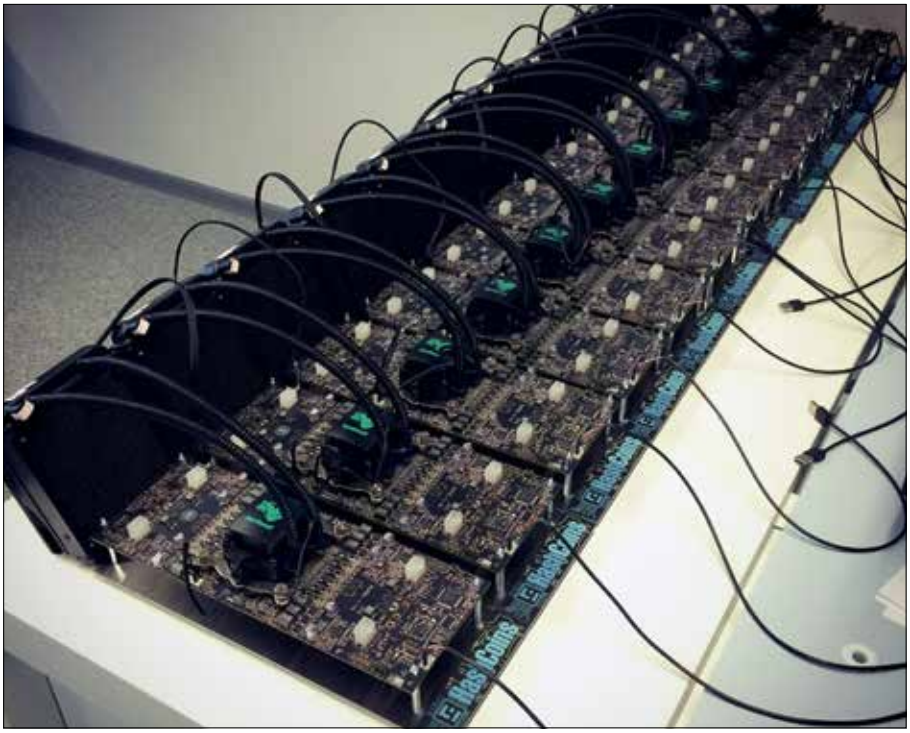
A digital or virtual currency maintains three basic pieces: an encryption used to secure each coin, a mathematical proof-of-work used to validate each coin's legitimacy, and a blockchain (database) that records transactions. The blockchain records a transaction history and posts it to a distributed ledger that creates data integrity and visibility to all participants. The desire to use this technology to support a completely free market system, not tethered to any state managed currency, drove the establishment of the segment leader, Bitcoin, in 2009.[2] All other available cryptocurrency outside of Bitcoin bears the generic label of "altcoin," that is, an alternative to Bitcoin, but operates on similar open-source code. Crucially, these currencies disrupt standard banking systems by introducing a means to establish peer-to-peer transactions without centralized ledger controls.

Traditionally, a ledger system that resided in one location stored the total of debits or credits transferred between individuals exchanging currency. While handwritten log books have given way to digital recordkeeping, middlemen (financial institutions) maintain these databases in central locations for easy tracking. However, this traditional method of currency exchange is vulnerable to cyber hacking as well as software and hardware malfunctions. The blockchain application addresses this vulnerability by generating a ledger of transactions verified, validated, and stored by a widely distributed network of autonomous peer computer systems (called mining computers). Various mining computers participate in these blockchains by confirming the transaction records between participant ledgers, and in doing so generate their own profit. A computing source compiles and produces the next block of transactions and mines (or gains) a digital currency token as reward for the effort of solving algorithms. Following the addition of a verified block (combined individual transactions), all computers across the network store the updated database on the distributed blockchain ledger.

The open (public) blockchain ledger effectively resides on thousands of computers participating in the minute-by-minute validation of the blockchain itself. In effect, the distributed blockchain stores and verifies the ledger and, in doing so, eliminates excess transaction fees and other negative externalities associated with single-ledger repositories, for example, the middleman, hacking, and corruption. Championed by a recent World Economic Forum report, blockchain technology allows for broader transparency and integrity in society, including the fight against bribery and corruption pertaining to monetary transactions because the ledger is public and exists in multiple duplicate copies.[3] The secure, encrypted, transparent, and distributed copies of the blockchain underlying cryptocurrency offer a dramatically new model for financial transactions.

While the international financial community certainly has shown both intrigue and aversion to the potential disruptions in world monetary markets, distributed ledger technology also introduces challenges pertaining to national security. The presence of various middlemen, such as financial institutions, afforded governments the ability to track and trace malign activity through the traditional financial system ledgers. With cryptocurrencies, reputable banks no longer validate an individual's credentials and record his information with each transaction. Rather, anonymity in cryptocurrencies protects point-to-point transactions captured between digitized wallets and encryption keys. This change in the traditional process for managing financial transactions undermines regulatory anti–money laundering efforts performed by financial institutions, which are intended to thwart players attempting to skirt sanctions and finance terror groups. While perhaps not immediately obvious to the casual observer, nonstate actor use and increasing state actor pursuit of cryptocurrencies extend the competitive space into the international financial domain and spotlight cryptocurrency as a national security issue that should concern the Department of Defense (DOD) and Intelligence Community.[4]

The rapid growth of weakly regulated financial and technology markets creates vulnerabilities for safeguarding the international financial system from malign actors. Hence, the nexus of crime, corruption, and terrorism finds refuge in these emergent financial systems.[5] Aside from the benefits of cryptocurrencies, which include providing an attractive means for malign actors to conceal illicit funding and business, and to earn currency by mining, the technology attributes alone attract malfeasance. While the distributed blockchain ledger remains



Mining kit based on golden nonce chip, May 20, 2015 (Alexandr Gromov)

resistant to cyber criminals, the storage of the digital coins (that is, private key encryptions) remains a system weakness.

While pointed out earlier that traditional ledger systems are vulnerable, theft of cryptocurrencies requires less hacking skill than penetrating the centralized ledger systems, which banks have hardened. Secure digital storage of the private and public key information associated with cryptocurrency exists outside the blockchain within individual computers, exchange markets, and businesses established to provide offline, or cold-storage. Similar to a brokerage house converting shares of a company into cash for a seller, cryptocurrency exchanges support the transition of the digital currency back into a fiat currency like the USD. Theft of the encryption keys for a coin gives a criminal carte blanche to spend it without the need for identification. Due to the need to secure the encryption keys from theft by hackers, some exchanges and separate businesses now exist to safeguard the encryption keys offline in the equivalent of digital safe deposit boxes. The introduction of these cryptocurrency technologies disrupts not only financial markets but also efforts to monitor and maintain the integrity of financial exchange. The anonymity of use, low barriers to entry, and weak regulation and limited legal jurisdiction in the cryptocurrency marketplace represent an opportune platform for illicit actors. The initial forays of criminal, corrupt, and terror networks into the cryptocurrency markets foreshadow the future challenges of starving large-scale, bad actors of funding.

Expanding the Competitive Space

Cryptocurrency transactions expand the international financial competitive space by creating an alternative to a fiat-based monetary system that skirts international financial mechanisms set to detect and intercept suspicious activities. Digital currencies also thwart U.S. Government sanctions policies, which rely on their effectiveness for tracking sales and trade conducted in USD. Outside of digital banking tools designed to disrupt rogue parties from receiving money, cryptocurrencies also negate military capabilities that are able to destroy physical cash stockpiles or target enemy financiers. The two effects of cryptocurrencies create a synergistic effect that allows rogue actors to cooperate in a secondary value transfer market impervious to the established world economic order. In doing so, cryptocurrencies present a viable means to unseat the USD as the recognized global reserve currency.

Upsetting the World Financial System and Unseating the USD as World Currency. While the USD has remained the dominant reserve currency following Bretton Woods, two nations have challenged the USD's dominance. In 2009, China and Russia called for the International Monetary Fund (IMF) to develop a new global currency, arguing that inflation and deficit spending in the United States would devalue reserves held in USD.[6] Today, the USD is still the most widely held reserve currency, and nearly two-thirds of all international trade is done in USD. Conducting trade in USD requires the use of the U.S. banking system to support the transactions, and all those transactions are subject to U.S. laws intended to protect international financial markets from bad actors. National security legislation that impacts the financial system includes anti–money laundering, countering the financing of terror, sanctions, the Foreign Corrupt Practices Act, and the USAPATRIOT Act.

The United States gains economic and diplomatic advantages through the strength of the U.S. financial markets in conjunction with the heavy use of the USD in world market trade. As a result, the United States can sustain large budget deficits, enforce sanctions, and dictate terms in international trade. From a strategic standpoint, competitors benefit by reducing U.S. dominance in world currency markets and international trade. Andrei Kostin, the head of Russia's second largest bank, VTB, indicated that Russia intends to find alternatives to the USD, suggesting, "This whip that the Americans use in the form of the dollar would then, to a great extent, not have such a serious impact on the global financial system."[7] Many rogue nations that desire to move money for malign intent echo Kostin.

Cryptocurrencies offer such an option for rogue actors: a new option for those

desiring alternatives to the USD and the affiliated banking and trade regulations. Referred to as a "money-laundering revolution" by a hacker and suspected terrorist's defense lawyer in New York City, nonstate actors reveal the benefits of functioning within the weakly regulated space of digital currency markets not tied to the USD.[8] Cryptocurrencies fueled illegal trade by criminal organizations on the "Silk Road," the online equivalent of a black market Amazon.[9] While not widely adopted, jihadist networks have raised funds through cryptocurrencies on Internet-based, crowdsource platforms. These platforms empower them to evade the international banking system stopgaps, which were instituted to hinder money laundering and prevent terror funding.[10]

With the technology and expertise at hand, a future digital economy is becoming a potential threat to the USD. The use of cryptocurrencies to evade traditional bad-actor countermeasures in the world financial system, and avoid the regulatory requirements of using the USD entirely, exposes burgeoning weakness in U.S. dominance of funding. The simultaneous migration from the USD, and the loss of the ability to control sanctions, would dilute a primary economic tool that the United States uses to curb confrontational behaviors, promote regime change, and limit access to products affiliated with national security.

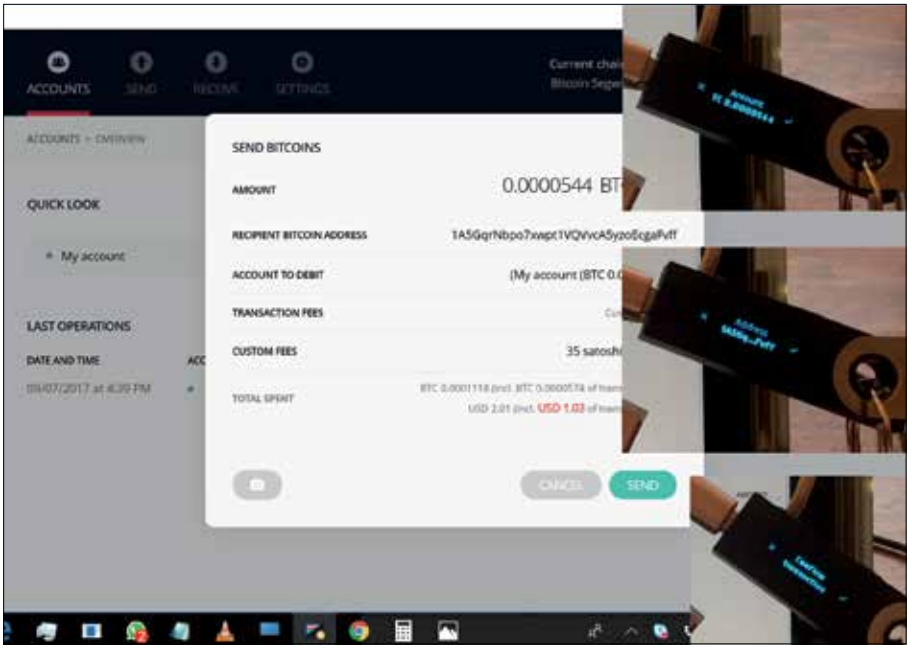
Avoiding Sanctions. Rogue regimes and revisionist powers are also aggressively seeking digital currency to erode the power of U.S. sanctions. Russia, Venezuela, Iran, and North Korea are actively exploring ways to implement national cryptocurrencies to circumvent the dollar and evade global oversight of financial transactions. The common theory is that the anonymity of cryptocurrencies will undermine U.S. hegemony by degrading its ability to control the flow of financial transactions in and out of sanctioned countries.[11] Direct cryptocurrency payments allow sanctioned countries to bypass financial controls established to enforce sanctions.

Russia, due to economic pressures applied to punish it for its actions in Crimea and chemical agent use, continues to adjust and develop means to evade sanctions. At the 2017 St. Petersburg International Economic Forum, President Vladimir Putin "announced that Russia was considering launching its own 'digital ruble' and praised the possibilities of virtual currencies."[12] Russian officials further suggested extending a supranational cryptocurrency for the BRIC nations (that is, Brazil, Russia, India, and China) as an alternative to the current U.S.-dominated economic system.[13] A BRIC digital trading block would offer not only an alternative currency but also the anonymity of financial transactions among the member nations—a model that rogue nations might establish to circumvent Western sanctions. Although Russia has yet to develop its own digital ruble, Moscow is reportedly behind Venezuela's new cryptocurrency with the purpose of helping an ally while using the experience as an experiment for future cryptocurrencies.[14]

Venezuela's new national cryptocurrency, the *petro* (*petromoneda*), is pegged to the value of oil. On the first day of its presale it raised over $735 million, with hopes of achieving $6 billion.[15] As noted by the Brookings Institution, "Foreign investors exclusively funded the presale; this rapid influx of capital could not have occurred by conventional means as Venezuela is subject to international sanctions."[16] Through the use of cryptocurrency, Venezuela effectively circumvented sanctions and accumulated foreign currency without meeting Western demands or addressing the underlying weakness of its national economy to attract traditional foreign direct investment. Furthermore, Venezuela may have brought short-term economic liquidity to a country suffering from hyperinflation and a contracting economy producing 40 percent less that it did 5 years ago.[17] If the petro succeeds, its digital model may serve as the example for other nations to follow.

Much like Venezuela, crypto technology may provide Iran a lifeline to counter existing sanctions in the short term. After the United States pulled out of the Joint Comprehensive Plan of Action, better known as the Iranian nuclear deal, and threatened additional sanctions, the value of the Iranian *rial* plunged to record lows against the USD, crippling Iran's economy.[18] Mohammad Reza Pourebrahimi, head of the economic committee in Iran's parliament, stated that he has already "obliged the Central Bank of Iran to start developing proposals for the use of cryptocurrency."[19] He added that Iran has been in talks with Russia to establish a cryptocurrency system to exchange goods between the two countries.[20] Short of a national cryptocurrency, major Iranian hotels recently announced they would begin to accept cryptocurrencies such as Bitcoin, Ethereum, and Bitcoin Cash, to encourage tourism and avoid U.S. sanctions.[21] The general discussion on the effects on the Iranian economy should not distract from the U.S. resolution to aggressively seek sanctions enforcement. As outlined by General Joseph Votel, the commander of U.S. Central Command, in a threat statement delivered to the House Armed Services Committee in February of this year, "Iran remains the major threat to U.S. interests and partnerships in the Central Region through support for numerous proxies, including Lebanese Hizballah operating in multiple countries, hardline Iranian-backed Shia Militia Groups in Iraq and Syria, and Iranian support-enabled Houthis in Yemen."[22]

North Korea began using cryptocurrencies to skirt U.S. sanctions in May 2017.[23] While not pursuing its own cryptocurrency, North Korea benefits by earning or stealing cryptocurrencies, which it then uses to purchase items required to support the regime. According to Recorded Future, a digital intelligence firm, North Korea has earned $15 to $200 million in USD-equivalent value (value range dependent on fluctuating prices) through legal cryptocurrency mining operations.[24] Steven Kim, a visiting research fellow at the Jeju Peace Institute in South Korea, acknowledged that "cryptocurrency is the ideal form of money for North Korea because it can be moved quickly and anonymously across borders and can be used to buy goods and services online or converted to hard currency."[25]



Bitcoin transaction with screenshots verifying amount and destination address, and physically confirming transaction, December 16, 2017 (FlippyFlink)

North Korea's illegal hacking activities are also of concern. North Korea has been accused of employing more than 7,000 hackers around the world focused on stealing cryptocurrencies, which has yielded tens of millions of dollars.[26] Given the extensive "maximum pressure" campaign undertaken by the Trump administration to limit North Korea's continued pursuit of weapons of mass destruction, its legal and illegal use of the unregulated cryptocurrency markets undermines these international efforts. Suggested by a former U.S. National Security Agency agent, "these coins are being turned into something—currency or physical goods—supporting North Korea's nuclear and ballistic missile program."[27] Like Venezuela and Iran, North Korea has demonstrated another method by which cryptocurrencies can undermine sanctions.

Although not under economic sanctions, Chinese participation in the realm of cryptocurrency should signal another competitive space that China views strategically. Maintaining control over its own currency, eroding the prevalence of the USD, and diminishing the strength of Western financial institutions all support the Chinese Grand Strategy released by the 19th Party Congress.[28] In recent years, China's leadership has routinely stated its desire to unseat the USD as the world's global currency.[29] Michael Collins, the deputy assistant director of the Central Intelligence Agency's East Asia Mission Center, warned that "Beijing does not want to go to war with the United States but is attempting to undermine Washington's global position by using all avenues available."[30] One of China's primary avenues is the domination of global trade through its "One Belt, One Road" economic initiative, which includes the cyber realm.[31] Thus far, China has indicated that it may develop its own state-backed form of digital currency but has been less supportive of decentralized initiatives, such as Bitcoin.[32]

China's intent to create a new world order by becoming a socialist superpower by 2050 includes an interest in cryptocurrencies. Previously observed is China's reluctance to pursue IMF approval of the *renminbi* as a world reserve currency; Chinese banks fear that decentralized digital exchanges would directly conflict with China's financial stability and control.[33] Regardless, China understands the power of the blockchain and, as of January 2018, has invested over 100 million dollars in research toward its application.[34] A globally accepted China-backed cryptocurrency could potentially weaken U.S. dominance in the global market, and significantly buttress Chinese Grand Strategy.

Combining Generates National Security Threats. A breakdown in international financial market transactions in USD and in the applications of international sanctions combine to generate a noteworthy national security threat. At the moment, malign actors hiding illegal transactions in cryptocurrency markets, or renegade companies skirting sanctions to generate short-term profit, represent a general nuisance to the overall maintenance of the international financial system. However, if rogue state actors cooperate to establish their own secondary market system of cryptocurrency transactions to trade among themselves, the effectiveness of using the global financial system to thwart these regimes would be significantly challenged.[35]

Unless rogue states coordinate to support all import and export transactions inside a single cryptocurrency, they would still need to convert open market cryptocurrencies to fiat currency. Currently, the cryptocurrency space displays wild fluctuations in value and demonstrates the instability of speculative investments and early market normalization. Since the value of each competing cryptocurrency remains purely based on investor confidence, currency prices tend to increase and decrease rapidly. Rogue nations releasing national digital currency tied to underlying assets presents a contemporary equivalent to the gold standard. If developed, trust among rogue actors in other digital marketplaces could allow for the free flow of illicit trade and funding among participant nations. Disconcertingly similar to the Cold War model, one could imagine this type of alternative market system leading to independent states choosing to operate in one or multiple marketplaces. This type of parallel digital market system challenges both nonkinetic (financial markets) and kinetic (DOD) means by which the United States might disrupt illicit actor funding.

As of July 28, 2018, open market cryptocurrencies represent under 1

percent of currency assets internationally, hence they do not represent an immediate financial market threat. However, this growing revolution in the establishment of cryptocurrencies harkens back to concepts introduced by Frederick Hayek in his 1976 essay, "Denationalisation of Money." Hayek proposed the need to remove the central bank monopoly over issuance of currency, which is the organizing principle of current cryptocurrencies. While the USD emerged as the stable world currency of choice, the functioning of U.S. Federal Reserve monetary policy as the de facto World Bank leaves many countries dissatisfied.

If rogue states coordinated their efforts to counter this actuality with support of a supranational cryptocurrency standard for trade and exchange, this technology could present a significant challenge to one of the primary tools used by the U.S. Government and the international community to counter continuously evolving gray area threats and activities of rogue nations and violent extremist organizations. The current instability in cryptocurrency marketplaces presents a window of opportunity for the United States to prepare for the revolution in international financial payment systems.

The Way Ahead

Advances in digital technologies and global connectivity benefit more than just bad actors in the financial landscape. Indeed, the United States participates (and thrives) in the cryptocurrency market. Well-established financial networks remain underpinned by a strong USD, which means decline of the USD is not a fait accompli. Despite increasing risk, there exist opportunities to maintain the USD's comparative advantage if actions are taken in the near term. Possible actions include advancing the U.S. capacity to countermand malign activity in the cyberspace domain of cryptocurrencies. To do so, the United States must reimagine its role in this new competitive financial space. Acknowledging U.S. vulnerabilities exposed by decentralized blockchain technology, the possibility of rogue national cryptocurrencies, and weakness in current digital currency regulations inform the way ahead.

Blockchain. As described in the new Joint Publication 3-12, *Cyberspace Operations*, the attributes of the cryptocurrency blockchain afford a position of marked advantage, representing key terrain in cyberspace.[36] Application of defensive practices involves understanding the ledger systems in cryptocurrency blockchains to detect pathways of bad actors and the establishment of a system to alert other legal actors, replicating the function of the current international banking system. Using offensive measures requires seizing or destroying the cryptocurrency of these actors in cyberspace, such as asset seizure or DOD kinetic strikes. Ultimately, DOD in particular must learn from the ways in which nonstate actors use cryptocurrencies in order to properly prepare to counter their inevitable use by other U.S. competitors.

National Cryptocurrency. Rogue nations establishing an adaptive parallel digital currency world marketplace directly challenge U.S. national security. The U.S. Government should consider the benefits of first-mover advantage to mitigate this potential. Establishing a stable USD form of cryptocurrency, backed by the fiat USD, would serve to retain U.S. command of world financial markets by allowing the near seamless conversion of this cryptocurrency back to fiat USD. Seizing this initiative would maximize the benefits of distributed ledger technologies and negate benefits of bad actors establishing parallel systems. Doing so would allow the United States to not only mitigate national security risks but also lead the world in countering corruption through financial transparency. Providing a reliable digital currency in the highly volatile cryptocurrency space allows the United States to preserve its positional and systematic financial advantage.

Regulation. Regardless of how much cryptocurrency matures and proliferates in the future, it already represents a significantly disruptive technology. The United States must position itself to continue to influence controls in the world financial markets. Leading the way in releasing a USD cryptocurrency affords the United States the ability to define the rules, regulations, and international oversite required to ensure the integrity of transitioning from a fiat to a cryptocurrency landscape. A crypto-USD, backed by the U.S. central bank, would enable the United States to offer higher levels of security regarding the cryptocurrency, complementing the benefits of openness generated with blockchain technology. The United States must reinvent guidelines in this cyberspace domain that aid the retention of a comparative advantage in the economic and financial elements of national power.

As the Department of Defense boldly marches toward innovative solutions to combat revisionist states and rogue regimes, the area of cryptocurrencies demands attention. With national security implications, the way ahead offers the potential integration of DOD cyberspace operations into the whole-of-government response. Significant defensive and offensive cyberspace capabilities exist should the U.S. Government remain ahead of the momentum building within this new financial space. The retention of the U.S. comparative economic and financial advantage should remain paramount to dominate the cryptocurrency space. **JFQ**

Notes

[1] Richard Best, "How the U.S. Dollar Became the World's Reserve Currency," *Investopedia.com*, September 23, 2016, available at <www.investopedia.com/articles/forex-currencies/092316/how-us-dollar-became-worlds-reserve-currency.asp>.

[2] "Frequently Asked Questions: Find Answers to Recurring Questions and Myths about Bitcoin," *Bitcoin.org*, available at <https://bitcoin.org/en/faq#who-created-bitcoin>.

[3] Don Tapscott and Alex Tapscott, *Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies* (Geneva: World Economic Forum, June 2017), 3, available at <www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf>.

[4] Kevin Coleman and Independent Software, "Cryptocurrencies—A Growing Issue for Military, Intel Agencies and Law Enforcement," *FifthDomain.com*, June 19, 2017, available at <www.fifthdomain.com/2017/06/19/cryptocurrencies-a-growing-issue-for-military-

intel-agencies-and-law-enforcement/>.

[5] Financial Action Task Force (FATF), *Emerging Terrorist Financing Risks* (Paris: FATF, October 2015), available at <www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>.

[6] Andrew Baston, "China Takes Aim at Dollar," *Wall Street Journal*, March 24, 2009, available at <www.wsj.com/articles/SB123780272456212885>.

[7] Simon Shuster, "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions," *Time*, March 20, 2018, available at <http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/>.

[8] Brett Forrest and Justin Scheck, "Jihadists See a Funding Boon in Bitcoin," *Wall Street Journal*, February 20, 2018, available at <www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601>.

[9] Kim Zetter, "How the Feds Took Down the Silk Road Drug Wonderland," *Wired*, November 11, 2013, available at <www.wired.com/2013/11/silk-road/>.

[10] Forrest and Scheck, "Jihadist See a Funding Boon in Bitcoin."

[11] Shuster, "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions."

[12] Owen Mathews, "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?" *Newsweek*, September 18, 2017, available at <www.newsweek.com/russia-finally-embracing-virtual-currencies-666794>.

[13] Ibid.

[14] Shuster, "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions."

[15] Jack Karsten and Darrell M. West, "Venezuela's 'Petro' Undermines Other Cryptocurrencies—and International Sanctions," Brookings blog, March 9, 2018, available at <www.brookings.edu/blog/techtank/2018/03/09/venezuelas-petro-undermines-other-cryptocurrencies-and-international-sanctions/>.

[16] Ibid.

[17] "Venezuela's Crypto-Currency: Salvation or Scam?" *The Economist*, March 17, 2018, available at <www.economist.com/the-americas/2018/03/17/venezuelas-crypto-currency-salvation-or-scam>.

[18] "Iran Rial Plunges to New Lows as U.S. Sanctions Loom," Reuters, June 24, 2018, available at <www.reuters.com/article/us-iran-economy-rial/iran-rial-plunges-to-new-lows-as-us-sanctions-loom-idUSKBN1JK0HZ>.

[19] Samburaj Das, "Iran and Russia Consider Using Cryptocurrency to Evade U.S. Sanctions: Report," CNN, May 21, 2018, available at <www.ccn.com/iran-and-russia-consider-using-cryptocurrency-to-evade-us-sanctions-report/>.

[20] Ibid.

[21] Joseph Young, "Major Hotels in Iran Accepting Deposits in Cryptocurrency to Avoid U.S. Sanctions," *Cryptoslate.com*, July 23, 2018, available at <https://cryptoslate.com/major-hotels-in-iran-accepting-deposits-in-cryptocurrency-to-avoid-u-s-sanctions/>.

[22] "Votel: Iran Is Major Threat to U.S. Interests in the Region," includes video, 2.11.06 (Washington, DC: United States Institute of Peace, March 5, 2018, updated March 14, 2018), available at <http://iranprimer.usip.org/blog/2018/mar/05/votel-iran-major-threat-us-interests-region>.

[23] Ralph Jennings, "North Korea Is Looking at Bitcoin to Escape Its Crippling Economic Sanctions," *Forbes*, December 19, 2017, available at <www.forbes.com/sites/ralphjennings/2017/12/19/north-korea-seeks-a-pile-of-bitcoin-to-escape-economic-sanctions/#77cf3c4e39ba>.

[24] Alex Ward, "How North Korea Uses Bitcoin to Get Around U.S. sanctions," *Vox.com*, February 28, 2018, available at <www.vox.com/world/2018/2/28/17055762/north-korea-sanctions-bitcoin-nuclear-weapons>.

[25] Jennings, "North Korea Is Looking at Bitcoin to Escape Its Crippling Economic Sanctions."

[26] Timothy W. Martin, Eun-Young Jeong, and Steven Russolillo, "North Korea Is Suspected in Bitcoin Heist," *Wall Street Journal*, December 20, 2017, available at <www.wsj.com/articles/north-korea-is-suspected-in-bitcoin-heist-1522303177>.

[27] Nicola Smith, "North Korea May Have Made as Much as $200 Million from Bitcoin, According to Expert," *The Telegraph* (London), March 5, 2018, available at <www.telegraph.co.uk/news/2018/03/05/north-korea-may-have-made-much-200-million-bitcoin-according/>.

[28] Dingding Chen, "China Has a New Grand Strategy and the West Should Be Ready," *The Diplomat* (Tokyo), October 31, 2017, available at <https://thediplomat.com/2017/10/china-has-a-new-grand-strategy-and-the-west-should-be-ready/>.

[29] Joe McDonald, "China Calls for New Global Currency," ABC News, March 24, 2009, available at <https://abcnews.go.com/International/story?id=7156932&page=1>.

[30] Saphora Smith, "China Is Waging a 'Cold War' Against the U.S., Says CIA Asia Expert," NBC News, July 21, 2018, available at <www.nbcnews.com/news/world/china-waging-cold-war-against-u-s-says-cia-asia-n893411>.

[31] "Planet China," *The Economist*, July 28, 2018, 7.

[32] Sara Hsu, "After Cracking Down on Bitcoin, China Contemplates Its Own Digital Currency," *Forbes*, October 19, 2017, available at <www.forbes.com/sites/sarahsu/2017/10/19/will-china-host-the-worlds-biggest-state-backed-digital-currency/#696ca5221231>.

[33] Sidney Leng and Xie Yu, "China Is Open to Idea of a Digital Currency, as Long as It's 'Efficient and Safe,'" *South China Morning Post* (Hong Kong), March 9, 2018, available at <www.scmp.com/news/china/economy/article/2136551/china-open-idea-digital-currency-long-its-efficient-and-safe>.

[34] Kevin C. Desouza, Chen Ye, and Xiaofeng Wang, "Is China Leading the Blockchain Innovation Race?" Brookings blog, July 19, 2018, available at <www.brookings.edu/blog/techtank/2018/07/19/is-china-leading-the-blockchain-innovation-race/>.

[35] Foundation for the Defense of Democracies, "Cryptocurrencies and Sanctions," Breakfast Conversation Panel, Center on Sanctions and Illicit Finance, Washington, DC, April 24, 2018.

[36] Joint Publication 3-12, *Cyberspace Operations* (Washington DC: The Joint Staff, June 8, 2018), I-6.

Jordanian Armed Forces soldiers engage targets with M-16s on hasty defensive line manned by U.S. and Jordanian troops near Amman, Jordan, April 26, 2018 (U.S. Army/David L. Nye)

Getting American Security Force Assistance Right

Political Context Matters

By Jahara Matisek and William Reno

If one accepts that the American military is the most powerful armed force in human history, why does it have a mixed record when it comes to building up foreign armies in weak states? With immense experience, capability, and resources, the United States should be able to train and develop competent armed forces in any host nation. Yet evidence over the past several decades has shown how difficult this task is. When a Senegalese general was asked why the United States struggled to create effective militaries throughout Africa, despite the United States (and other countries) committing tremendous resources (for example, funding, equipment, trainers/advisors, among others), he explained, "The logic of their politics will show you the quality of their military."[1] His remark should not come as surprise, yet in interviews with officials that oversee (and conduct)

Major Jahara Matisek, USAF, is an Assistant Professor in the Department of Military and Strategic Studies at the U.S. Air Force Academy. Dr. William Reno is a Professor in the Political Science Department at Northwestern University.

Soldier with 1st Security Force Assistance Brigade's 3rd Squadron meets with Afghan Command's senior enlisted leader (left) during routine fly-to-advise mission, Forward Operating Base Altimur, Afghanistan, September 19, 2018 (U.S. Army/Sean Kimmons)

security force assistance (SFA), there is a massive disconnect between what is believed possible and what can actually be accomplished given the political context within each country.[2] This highlights a substantial problem with Western SFA: it is too focused on building an army in the absence of a viable state that has the institutional capacity and political willpower to sustain that army.

There are several sides to the SFA debate. First, there are critics who view SFA as enabling host-nation militaries to engage in more violence and human rights abuses—an increase in capacity, but without proper discipline in its use.[3] In this vein, some argue that SFA in the form of International Military Education and Training and the Countering Terrorism Fellowship program leads to an increase in coups d'état.[4] Others argue that military assistance to Colombia played a role in increasing political violence and undermined domestic political institutions as pro-government paramilitaries indirectly benefited from this assistance.[5] These arguments rest on the assumption that any aid to militaries in weak states does more harm than good.

Other scholars are less critical of SFA and emphasize the ways that it can be used judiciously as an incentive for desired performance. Kristen Harkness, for instance, contends that SFA should be provided on a "carrots-and-sticks" basis, where host-nation governments are conduced into not politicizing their armed forces by reforming them to be meritocratic in place of recruitment and promotion on the basis of loyalty and patronage.[6] This approach relies on assumptions that recipients of SFA will respond to incentives in predictable and beneficial ways. Others contend that SFA is effective only when there is a substantial donor commitment (from the United States, for example) alongside a host-nation government that has national interests closely aligned with the donor patron state.[7] There are valid concerns, however, that all the money and energy spent on SFA without addressing internal political problems in a weak state will just result in the creation of a Fabergé egg army: expensive to build but easy to crack.[8] While SFA may promote desired outcomes in some recipient states, the resources and advice that donors provide in weak states just exacerbate the underlying problems already present.

The Fabergé egg army problem points to the central importance of political context: weak states have governments that lack legitimacy and a national sense of identity. Such regimes usually provide few public goods and services and are prone to significant internal violence.[9] The political environment encountered in this type of weak state is notable for numerous embedded contradictions

between national- and local-level politics. This is where the formalities of the state shift into the informal, as state authority is exercised through a series of bargains with local powerbrokers rather than on the basis of performance legitimacy gained through providing services and protection to citizens. These alliances with various powerbrokers such as local strongmen, warlords, and militias usually are precarious. In some countries, these bargains extend into the realm of illicit commercial activities, such as drug-trafficking and financial frauds, as high officials turn a blind eye to (and themselves profit from) these activities in return for political support.[10] These opaque relationships dictate—to varying extents—the development of political coalitions and negotiations that leads to the mobilization of power bases that are coordinated through different forms of authority and legitimacy.

A substantial problem develops within this context when Western militaries attempt to provide SFA and expect their partners to undertake reforms as a condition for this support. Many times, the actual SFA providers on the ground have to navigate local politics that make by-the-book operational procedures impossible. This leads many SFA troops on the ground to develop ad hoc relations between various armed actors and government factions to achieve order and maintain relative safety. This is a particularly difficult situation for the SFA provider when some of the government officials who are supposed to play central roles in assistance programs are themselves implicated in the kinds of activities that SFA is meant to address.[11] SFA is made worse when there is a strategic disconnect from this on-the-ground experience, which can range along the spectrum from merely establishing military-to-military relations all the way to building a new standalone army. Each presents its own particular costs, risks, and benefits. Various elites from the national down to local level, including people whose behavior and interests contribute to the problems that SFA is supposed to address, have an incentive to utilize SFA for their own purposes, either as patronage to reward loyalists or to eliminate rivals.

Almost by definition, many of the weak state's government officials, military officers, police, and others who are the formal state's main interlocutors with the United States and other SFA providers can at the same time be involved in the very activities and organizations that SFA troops identify as the problem. It is problematic when Western advisors have to train Iraqi police and personnel who are connected to sectarian militias. This frustration is expressed well in a video of a U.S. Army sergeant berating Iraqi police trainees for their loyalties to sectarian militias instead of to their country.[12] SFA in the hands of these people may have the effect of increasing the power of particular militias at the expense of the effectiveness and legitimacy of the police or army as a whole. Likewise, local government officials who oversee SFA program beneficiaries in some cases are the same people who are involved in criminal networks and large-scale corruption.[13] The risk is that their SFA connections likely empower these people and their informal strategies that weak state officials use to exercise authority at the expense of long-term donor aims. The critical problem for SFA in these cases is that success would have to involve a massive overhaul of the way the recipient state is structured, not just a few key reforms. This would amount to a state-building enterprise, whether it is acknowledged or not.

Challenges of Improving SFA

The United States and its allies, such as the United Kingdom (UK), are not interested in huge state-building projects. Instead, they are adapting to the demand for more SFA in these difficult political contexts. Each has recently created a specific unit: the United States is standing up six security force assistance brigades (SFABs) and the British are developing two new specialised infantry battalions (SIBs)—designed around strengthening their SFA abilities.[14] These programs essentially focus their training and assistance on creating pockets ("enclaves") of effective local forces focused on specific tasks. Despite these well-intentioned efforts, SFABs and SIBs will struggle in future SFA efforts for three reasons.

First, there are substantial bureaucratic hurdles impeding SFA as an important mission set. Western militaries rarely allow their best military personnel to be involved in SFA activities because it is treated as a "backwater" that damages career advancement and promotion opportunities. Spending long periods of time in sub-Saharan African countries in an advisory role is not a good formula for rapid advancement through the ranks. Historically, there has been a tendency to treat such SFA efforts as a low priority relative to conventional warfare. Worse, military personnel systems in the United States and UK are unwilling to reward those who excel in their SFA duties.[15] Even the well-intentioned AfPak Hands program, with an emphasis on nation-building and improving SFA to Afghanistan and Pakistan, was mismanaged, and many Servicemembers who volunteered for it lamented how it hurt their careers.[16]

Second, military advisor units are not designed to deal with the "bad" politics in a fragile state. Despite what Western politicians might say, the problems of a weak state in the periphery are not treated as an existential threat, leading to half-hearted attempts at SFA to contain a security problem instead of addressing the root causes (for example, bad host-nation governance). The average Western military would rather worry more about developing AirLand Battle concepts and practicing combined arms maneuver for war with a near-peer than to concern its military with the parochial problem of SFA. This is because tactics and capabilities must be carefully adapted to the social milieu of a failed state, which requires Western advisors on the ground to know the language and culture so that they can read the "political terrain." This can take years to properly develop. Those who do spend time to meet local people, acquire a local language, and learn about the intricacies of politics do so at the risk of not tending to other priorities that will help them advance up the career ladder.

Moreover, the dedicated operator may be surrounded by "bad apples" who are assigned to these lower priority missions.

Third, little strategic thinking is put into SFA. It is assumed that resources, in terms of advisors provided and host-nation troops trained and equipped, will generate the desired product—a host-nation army capable of marching and shooting straight. However, such SFA efforts to provide the "ABCs" of military training to an army in a fragile state is a dubious effort because the organization of politics in a weak state has considerable overlap. There are numerous unconventional ways of asserting authority and legitimacy in political and military affairs. Instead of formal government structures dictating politics, the exertion of control is informally conducted through networks, surveillance, and kinship. The destabilizing aspect of SFA is that Western militaries typically try to create an apolitical host-nation military designed for a liberalized democratic state. However, this can create substantial problems for the viability of the host-nation government, especially if the newly trained military believes itself to be better at governing. This problem arose in Gambia with the aborted coup of Lamin Sanneh, a reform-minded Gambian officer who earned a master's degree at the National Defense University in Washington, DC. Upon returning to Gambia, Lieutenant Colonel Sanneh concluded that serving his president, who was involved in massive corruption and drug-trafficking, was at odds with his professional military education.[17]

In this article we argue that successful SFA has little to do with doctrinal approaches or the type or form of training provided to host-nation militaries. Instead, effective SFA requires overt signals of commitment from Western governments to a targeted set of elites in the weak state. This requires a willingness by Western leaders to provide long-term support to reform-minded people in fragile governments as long as reforms are undertaken. Such actions facilitate the removal of these militaries from the bad politics of the state. Successful SFA must be tied to strengthening the state and its politics toward its own efforts at long-term state-building without trying to forcefully push democratization, which can promote violence and destabilization.[18] This is precisely why an Ethiopian general relayed in an interview, "If we copied your military [U.S. Armed Forces] it would be dangerous to Ethiopia."[19] Learning about and acting on the nuances of a complicated political context is an information-intensive exercise and requires adjusting SFA to fit specific contexts so that a more capable military is viewed as compatible to political and societal elites. Pursuing such an alternative path may mean accommodating some of the practices and priorities of local elites that are not in total alignment with the way the United States wants to conduct SFA.

Finally, Western ideas of a subservient military in such a weak state context might do more harm than good. Due to the nature of violence and politics in this context, known as limited access orders, military elites generally behave as co-equals with other political actors and societal elites.[20] Any attempt to make these actors subservient without stronger institutions, including checks and balances, may tip the balance of power, leading to fragmentation in the government and military. If the United States can adapt SFA to the realities of such a political context—specifically avoiding the common pitfalls of building an army in a weak state—then smarter SFA could be provided to build a stronger state with an effective military.

Weak State or Weak Army? The Three SFA Traps

Engaging weak states is in America's national interest. As first identified in the Bush administration's 2002 National Security Strategy (NSS), "weak states . . . pose as great a danger to our national interests as strong states."[21] Such language about weak states was recently updated by the Trump administration in the 2017 NSS to indicate that the United States "will give priority to strengthening states where state weaknesses or failure would magnify threats to the American homeland."[22] Weak states provide environments conducive to insurgency and terrorism and can create humanitarian crises (for example, refugees) that contribute to domestic political instability (extremist domestic politics caused by an immigration influx).[23] Yet there is almost an inherent moral hazard with helping prop up an army that the host-nation government cannot afford, sees as a threat, or is treated as something to manipulate toward its own consolidation of power. This observation points to three types of SFA traps, which are best illustrated with the cases of Afghanistan, Somalia, and Iraq.

Unaffordable. Afghanistan encapsulates the issues facing a country that cannot afford an army it needs to maintain the illusion of control and stability. A 2014 Special Inspector General for Afghanistan Reconstruction report noted that without Western combat troops, the Afghan government would need to maintain a security force of over 370,000 personnel to control and defend the country from Taliban infiltration. The report also indicated that it would cost over $5 billion annually for the Afghan government to maintain a military that large. This is highly problematic given that this would take up the majority of the Afghan budget, leaving only enough to fund one-third of other government functions (for example, infrastructure, civil servants, among others).[24] More realistically, the Afghan army will only exist if the United States and other donors pay for it. Open-ended foreign financing means Afghans have no incentive to make sacrifices and reforms needed to sustain such a security force. The smart Afghan will just sit back, letting the West subsidize bad governance. An Afghan military without a state is not a viable future or desirable outcome, yet current policies do not provide incentives for Afghans to create a stronger state.

The United States and its allies have learned that the Afghan National Army (ANA) can be effective when Western combat troops are attached, but these ANA units become militarily ineffective when operating on their own. In short, the ANA works well when Western

Forces Armées Nigeriennes soldier watches his sector in training mission during Flintlock 2018 exercise, at Agadez, Niger, April 17, 2018 (U.S. Army/Mary S. Katzenberger)

troops operate alongside as "co-combatants." When the ANA must operate independently, they fall apart. The only exception are the U.S.-trained Afghan army commandos, who are elite soldiers capable of rapidly deploying and handling crises.[25] Unfortunately, this is not enough for the vast expanses and rough terrain of Afghanistan. The harsh reality is that, as of late 2017, the Afghan government only controls 30 percent of the country, which are districts with Western troops assigned to ANA units.[26] Thus, the survival of Kabul depends on foreign troops being attached to as many ANA units as possible and its few elite commando units. But there are long-term implications because few (if any) Western governments are willing to make such an open-ended commitment of SFA to an Afghan government that is perceived as weak, corrupt, and incapable.[27] The fact that the Afghan government cannot afford the sizable army needed to maintain order and stability or have an ANA operate independently makes the viability of the Afghan state tenuous at best for the foreseeable future.

Threatening. It makes sense that most governments, weak ones especially, are most worried about soldiers with guns. This problem is the *civil-military problematique*, where the "military [is] strong enough to do anything the civilians ask them to with a military subordinate enough to do only what civilians authorize them to do."[28] In practical terms, this is a serious issue in Somalia, where clan politics dominate how different components of the Somali National Army (SNA) and other security organizations are configured. The problem becomes more complex when one acknowledges the reality that many Somali politicians perceive different factions of the military as a threat to their personal rule and their family clan ties. In response to perceived threats, they empower their favored armed groups (state-sanctioned and nonstate) to attack other components of the government and security institutions. This problem persists despite American military assistance, from 2007 to present, totaling over $2 billion, with over 1,500 SNA troops trained.[29] Since 2010, the European Union Training Mission in Somalia has been providing mentoring and advising to the SNA.[30] Despite such aid, pathological "clannism" politics continues to pervade Somali security institutions, where various SNA factions are more loyal to their kinship groups than the national government.[31]

The establishment of a Turkish military training base in Mogadishu further complicates SFA matters.[32] Turkey's presence provides a different venue for the politicization of the SNA with ties to Turkish strategic interests. Subsequent interest in Somalia's military on the part of the governments of Qatar, the United Arab Emirates (UAE), and others

complicates the situation even more, especially as ideological and strategic strains develop among these various funders. For example, SNA troops assaulted UAE troops at their military training center in Mogadishu, partially under the premise to loot—but also to send a signal to the UAE about its decision to build a military base and port in the secessionist state of Somaliland.[33]

The only credible Somali partner on the ground appears to be the Danab ("Lightning"), an elite Somali commando unit specifically trained by U.S. Special Forces. Its military effectiveness against al-Shabaab appears to correlate with its ability to transcend bad Somali politics by having a meritocratic mixed-clan organization.[34] However, its ability to operate as an enclave outside of predatory Somali politics is only possible with the presence of U.S. military trainers. Danab troops are housed in a compound separate from Somali politics and society. Thus, Danab military effectiveness is a function of its removal from the negative influences of what is the façade of a government in Mogadishu and the clan-based politicians who serve in official posts. Is this sustainable, or does the United States and its allies have to make the entire SNA like the Danab? That would simply make this militia an extension of U.S. military training and advising rather than a part of a real Somali security force. Worse, what will the Danab do if the U.S. military leaves? Will the Danab be a threat to the Somali government if it is the only competent organization in Somalia? Already, there have been multiple incidents of SNA components and other Somali security institutions getting into gunfights with one another and against the Danab.[35] This problem reflects the on-the-ground reality that each armed faction is vying for control of the government and also that each faction regards others as more of a threat than a viable component of a collective Somali state-building effort. Providing SFA to Somalia, when there is so much in-fighting, is troubling when al-Shabaab should be viewed as the bigger threat since it "still controls large swathes of Somalia" as of April 2018.[36] Indeed, it appears that al-Shabaab is the most effective military force and state-builder in Somalia, particularly considering the limited resources at its disposal.

Politicized. The failure and eventual collapse of the Iraqi military after U.S. trainers left in 2011 is not an indictment against Iraqi soldiers and their willingness to fight the so-called Islamic State (IS), but highlights a failed political system. The Iraqi prime minister, Nuri al-Maliki, started packing the military with loyalists and politicized (and personalized) different components of the Iraqi security forces.[37] Such sectarian favoritism led to fragmentation of the Iraqi military when IS started conquering territory in 2013, as Iraqi army units chose to flee instead of fighting small contingents of IS fighters.[38] Since Maliki explicitly chose Shia constituents over Sunnis, this undermined Iraqi military cohesion.[39] Disenfranchised Sunnis found it relatively easy—besides for basic survival—to swap alliances from Baghdad to IS because they had been abandoned politically and materially.[40]

When the U.S. military finally came to the rescue of the Iraqi government, it was only because IS fighters were within 15 miles of the Baghdad airport in late 2014.[41] When the United States (and other Western allies) deployed their combat troops and advisors alongside Iraqi military units, they were able to help the Iraqi army overcome politicized and sectarian splits. This improvement in Iraqi military effectiveness was a function of these troops operating outside of the corrosive sphere of sectarian politics that had undermined unit cohesion, loyalty, and morale. Beyond politicians helping to hollow out the Iraqi army, various commanders were pocketing funds meant for their units.[42] For instance, an American advisor working in Baghdad in early 2015 was appalled to discover that most Iraqi troops hurt in anti-IS combat operations were "kicked out of the military because their commanders did not want to pay their medical bills out of their own pockets."[43] No wonder so many Iraqi troops fled when faced with the prospect of fighting IS.

The greater failure of the Iraqi army was based on Maliki's decision to target Sunni protestors in Anbar Province who complained that their government was attacking them and reneging on earlier agreements to incorporate more Sunnis into the Iraqi security forces.[44] Given that these forces were attacking them, some people allowed their neighborhoods to fall into the hands of IS fighters. This outcome was more a product of bad political decisions by Maliki to empower loyalty over competence, which meant aggressive behavior toward a sectarian community rather than empowering the fighting abilities of the Iraqi army.[45]

The only bright spot was the emergence of the "Golden Division" in Iraq's Counter-Terrorism Service, which played a substantial role in liberating IS-held territories in Iraq with minimal U.S. assistance. The Golden Division was effective because its origins were based on being trained outside of the contentious political environment after 2003. Moreover, its leadership, specifically Lieutenant General Abdul-Wahab al-Saadi, had "zero tolerance for sectarianism," which prevented his units from being politicized and personalized by corrupt Iraqi politicians.[46] The performance of the Iraqi military during the rise and fall of the IS "caliphate" (2013–2017) suggests that the Iraqi military is capable of being effective in its own enclave when separated from corrosive Baghdad politics.

However, positive Iraqi military outcomes either requires "babysitting" by foreign military personnel or exemplary leadership as seen in the Iraqi Golden Division. How can the Iraqi military institutionalize such nonsectarianism and robust leadership? Or is the Iraqi military only bound to be further politicized by ambitious Iraqi politicians seeking to consolidate their own power through divide-and-rule strategies? The future looks difficult as Iranian-backed militias in Iraq, known as the Popular Mobilization Forces (PMF), have been integrated into the formal structures of the Iraqi military.[47] The PMF will likely play a disruptive role in building Iraqi security institutions devoid of politics.

The PMF represent a considerable challenge, as some Iraqis perceive them as serving the interests of sectarian political

parties and individual strongmen rather than a broad Iraqi national interest. Some PMF units even fly the flags of sectarian political parties alongside the national flag, which raises concerns among some Iraqis that these elements of the national army are interested in protecting only their supporters, as opposed to all Iraqi citizens.[48] The problem for SFA in this context concerns how to ensure that skills and supplies are not transferred from the army to sectarian militias. This is a hard distinction to make when the United States, Iran, and many neighboring countries are all vying to influence Baghdad in different directions.

Adjusting SFA to the Weak State Paradigm

Each of these specific (and overlapping) problems in the armies of Afghanistan, Somalia, and Iraq is illustrative of the American SFA-paradox: helping weak governments create effective security institutions that will remain strong without American involvement. If history is any guide, the success of American SFA hinges on long-term commitments to support state institutions alongside the building up of a host-nation military. However, with the rise of globalized insurgencies and collapsed states, domestic audiences in the West are unwilling to back politicians who suggest open-ended commitments to countries that seem so dissimilar to their own.[49] The idea of a contemporary American strategy that emulates a post-1945 commitment seems untenable and unsellable. At the same time, experience shows us that the stationing of substantial numbers of U.S. troops—with no timeline for withdrawal—in Germany, Italy, and Japan (and South Korea after the Korean War) illustrates a path toward success that no politician or military leader dares now suggest.

The alternative solution is a bitter pill to swallow, but is more grounded on the harsh realities of politics in weak and fragile states. While interviewing American and British military personnel who conducted SFA in weak states, they consistently talked about their roles in helping develop tactical capabilities and how important they believed it was for these militaries to develop self-sufficiency and military effectiveness.[50] However, there is substantial naiveté in believing that Western SFA can overcome deep-rooted political problems that prevent long-term defense-institution building (DIB). In fact, an overemphasis on tactical expertise and operational education and training in SFA does a disservice to most militaries in a weak state precisely because this may not be sustainable given the political context—whether for budgetary reasons, issues of civil-military relations, and/or politicization of security forces. What good is a tactically proficient military, with expensive weaponry and considerable training, in a context where state officials lack political willpower and capacity to support such a force? This is a recipe for the expensive to build, yet easy-to-break Fabergé egg army. These problems suggest that American SFA in weak states needs to be just as focused on doing politics as that of providing specific military training.[51]

Without developing the necessary political and social space for militaries to professionalize free from the political pathologies of most weak states, no amount of aid or assistance will remake this context, short of a massive state-building effort. Context matters and SFA should be adapted to it. If we return to the thoughts of the Senegalese general, the U.S. military must be willing to play a positive role in developing good politics in the host nation so as to produce a positive outcome—a competent and effective host-nation military that behaves in a benign fashion. This is a discomforting position for Western military personnel who are taught to remain apolitical. Yet in underdeveloped weak states, political cohesion is at a premium, and if this requires the development of militaries that are more politically involved in state-building, it is better to have them engaged in positive state-building rather than being used as tools against domestic rivals. Such a blended form of civil-military relations might upset those who subscribe to Samuel Huntington's vision for dichotomous relations between the Soldier and the State.[52] However, some weak African states, such as Rwanda, Uganda, and Ethiopia, have managed to develop highly effective militaries

Third Air Force/17th Expeditionary AF commander (right) walks with 323rd Expeditionary Reconnaissance Squadron commander toward MQ-9 Reaper, at Nigerien Air Base 101, Niger, October 19, 2017 (U.S. Air Force/Joshua R.M. Dewberry)

precisely because their armies have "partnerships" with the state and are strategically integrated into the "shared vision" for state-building.[53]

Conclusion

The basic dilemma for providing SFA to weak governments is that the beneficiaries are often implicated in the activities that this assistance is meant to address. In Iraq, sectarian militias undermine national unity and Baghdad's legitimacy. SFA cannot build a sustainable Iraqi military (or properly conduct DIB) in such a context. Corrupt officials in Afghanistan do not need the ANA to defend them from the Taliban because America subsidizes it through SFA. Practitioners can think of any number of examples of this sort occurring right now throughout Africa and the Middle East.

It is tremendously hard to sustain a Western-styled military that is professional and capable in a fragile state. Many host-nation leaders lack the political willpower and capacity to utilize the benefits of SFA in this context, at least beyond distributing SFA as patronage. At present, the best the U.S. military can do in these situations is to build a militia that is insulated from the bad politics of the state and to use that militia for counterterrorism or other specific tasks that serve American national interests. Moving beyond this situation requires a much more intensive political engagement with these states. It would include more coercive measures to force reforms and to install honest partners. This comes with dangers because the American public is reluctant to return to the failed politics of state-building. Attempts to install Western-friendly officials in weak states will become an American-made problem, and these leaders will likely be criticized by opponents for serving Western interests.

These problems present real risks. But there are some pathways out of this dilemma, through limited engagements, savvy political maneuvering, and patience on the part of U.S. officials and practitioners. This requires deep knowledge of local political contexts and familiarity with key actors. These qualities in turn rest on the willingness of U.S. planners and politicians to remain focused on these countries, pursue consistent policies, and provide the necessary career rewards to the professionals on the ground who devote substantial time and energy to getting this job done.

This sounds easy on paper, but success will only come with national security leadership making SFA a priority, which seems unlikely since the 2015 shuttering of the *DISAM Journal of International Security Cooperation Management*, a Defense Department–funded journal that focused on improving SFA.[54] Future SFA success rests on supporting the necessary intellectual foundations and frameworks needed to develop and sustain commitments to militaries *and politicians* in weak states. Failure to do so will only lead to America building more expensive Fabergé egg armies that easily break when the U.S. military leaves. JFQ

Notes

[1] Authors' interview, Dakar, Senegal, August 14, 2017.

[2] Authors' interviews, Pentagon, July 26–29, 2017; authors' interviews, U.S. Africa Command (Stuttgart, Germany), August 1–5, 2017.

[3] Kersti Larsdotter, "Security Assistance in Africa: The Case for Less," *Parameters* 45, no. 2 (2015), 25–34.

[4] Jesse Dillon Savage and Jonathan D. Caverley, "When Human Capital Threatens the Capitol: Foreign Aid in the Form of Military Training and Coups," *Journal of Peace Research* 54, no. 4 (2017), 542–557.

[5] Oeindra Dube and Suresh Naidu, "Bases, Bullets, and Ballots: The Effect of U.S. Military Aid on Political Conflict in Colombia," *Journal of Politics* 77, no. 1 (2015), 249–267.

[6] Kristen A. Harkness, "Security Assistance in Africa: The Case for More," *Parameters* 45, no. 2 (2015), 13–24.

[7] Stephen Biddle, Julia Macdonald, and Ryan Baker, "Small Footprint, Small Payoff: The Military Effectiveness of Security Force Assistance," *Journal of Strategic Studies* 41, nos. 1–2 (2018), 89–142.

[8] Jahara Matisek, "The Crisis of American Military Assistance: Strategic Dithering and *Fabergé Egg* Armies," *Defense & Security Analysis* 34, no. 3 (2018), 267–290.

[9] Robert I. Rotberg, ed., *State Failure and State Weakness in a Time of Terror* (Washington, DC: Brookings Institution Press, 2004).

[10] William Reno, *Warlord Politics and African States* (Boulder, CO: Lynne Rienner Publishers, 1999); Vanda Felbab-Brown, Harold Trinkunas, and Shadi Hamid, *Militants, Criminals, and Warlords: The Challenge of Local Governance in an Age of Disorder* (Washington, DC: Brookings Institution Press, 2017).

[11] William Reno, "The Politics of Security Assistance in the Horn of Africa," *Defence Studies* 18, no. 4 (2018), 498–513, available at <www.tandfonline.com/doi/full/10.1080/14702436.2018.1463819>.

[12] "U.S. Army Sgt. Gives Iraqi Police a Telling Off," video, 5.36, November 25, 2010, available at <www.youtube.com/watch?v=Cj6AXvkBnv4&t=10s>.

[13] Fieldwork, Baghdad, Iraq, and Kurdistan, April 9–26, 2018.

[14] U.S. Army Public Affairs, "Army Creates Security Force Assistance Brigade and Military Advisor Training Academy at Fort Benning," *Army.mil*, February 16, 2017, available at <www.army.mil/article/182646/army_creates_security_force_assistance_brigade_and_military_advisor_training_academy_at_fort_benning>; Michael Fallon, "Strategic Defence and Security Review—Army: Written Statement—HCWS367," *UKParliament.uk*, December 15, 2016, available at <www.parliament.uk/written-questions-answers-statements/written-statement/Commons/2016-12-15/HCWS367>.

[15] Authors' interviews with American and British personnel involved with Security Force Assistance, February 7, 2018, and July 17, 2018.

[16] Thomas E. Ricks, "It May Be the Top Personnel Priority of the Chairman of the Joint Chiefs—But Is the AfPak Hands Program Flopping?" *Foreign Policy*, April 8, 2011, available at <https://foreignpolicy.com/2011/04/08/it-may-be-the-top-personnel-priority-of-the-chairman-of-the-joint-chiefs-but-is-the-afpak-hands-program-flopping/>; Hans Winkler and Robert Kerr, "AFPAK Hands: Time for Strategic Review?" *Small Wars Journal*, June 4, 2018, available at <http://smallwarsjournal.com/jrnl/art/afpak-hands-time-strategic-review>; authors' interviews with AfPak Hands members, 2015–2018.

[17] Jeffrey Meiser, "The Dilemma of an African Soldier," *War on the Rocks*, January 26, 2015, available at <https://warontherocks.com/2015/01/the-dilemma-of-an-african-soldier/>.

[18] Julia Leininger, Sonja Grimm, and Tina Freyburg, eds., *Conflicting Objectives in Democracy Promotion: Do All Good Things Go Together?* (New York: Routledge, 2017).

[19] Authors' interview, Addis Ababa, Ethiopia, August 7, 2017.

[20] Douglass C. North et al., eds., *In the Shadow of Violence: Politics, Economics, and the Problems of Development* (New York: Cambridge University Press, 2013).

[21] *The National Security Strategy of the United States of America* (Washington, DC: The White House, September 17, 2002).

[22] *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), 39–40.

[23] Edward Newman, "Weak States, State Failure, and Terrorism," *Terrorism and Political Violence* 19, no. 4 (2007), 463–488.

[24] John F. Sopko, *Special Inspector General for Afghanistan Reconstruction: Quarterly Report to the United States Congress* (Arlington, VA: Special Inspector General for Afghanistan Reconstruction, July 30, 2014).

[25] Shashank Bengali, "These Are Afghanistan's Best Troops: The U.S. Is Backing a Plan to Create Many More of Them," *Los Angeles Times*, December 10, 2017, available at <www.latimes.com/world/asia/la-fg-afghanistan-special-operations-20171209-htmlstory.html>.

[26] Shoaib Sharifi and Louise Adamou, "Taliban Threaten 70% of Afghanistan, BBC Finds," BBC, January 31, 2018, available at <www.bbc.com/news/world-asia-42863116>.

[27] Vanda Felbab-Brown, "The Weak, the Bad, and the Ugly: Policy Options in Afghanistan," Brookings blog, October 28, 2008, available at <www.brookings.edu/opinions/the-weak-the-bad-and-the-ugly-policy-options-in-afghanistan/>; Alicia P.Q. Wittmeyer, "What Went Wrong in Afghanistan?" *Foreign Policy*, March 4, 2013, available at <http://foreignpolicy.com/2013/03/04/what-went-wrong-in-afghanistan/>; R. Jeffrey Smith, "American Leaders Persistently Ignored Warnings That Afghan Government Corruption Would Undo Rebuilding," Public Radio International, October 18, 2016, available at <www.pri.org/stories/2016-10-18/american-leaders-persistently-ignored-warnings-afghan-government-corruption-would>.

[28] Peter D. Feaver, "The Civil-Military Problematique: Huntington, Janowitz, and the Question of Civilian Control," *Armed Forces & Society* 23, no. 2 (1996), 149–178.

[29] "Security Aid Data," Security Assistance Monitor, April 1, 2018, available at <http://securityassistance.org/data/country/military/country/2000/2017/all/East%20Africa//>; "Trainees Data," Security Assistance Monitor, April 1, 2018, available at <http://securityassistance.org/data/country/trainee/country/2000/2017/all/East%20Africa//>.

[30] Common Security and Defence Policy, "European Union Training Mission–Somalia," European Union External Action, March 2018, available at <www.eutm-somalia.eu/download/1125/>.

[31] Colin D. Robinson, "The Somali National Army: An Assessment," *Small Wars & Insurgencies* (forthcoming).

[32] Tom O'Connor, "Turkey's Military to Move into Somalia after Backing Qatar in Gulf Crisis," *Newsweek*, August 7, 2017, available at <www.newsweek.com/turkey-military-move-somalia-backing-qatar-gulf-crisis-646836>.

[33] "UAE to Train Somaliland Forces Amid Somalia Rift," *Middle East Monitor* (London), March 16, 2018, available at <www.middleeastmonitor.com/20180316-uae-to-train-somaliland-forces-amid-somalia-rift/>; "Somali Forces Clash with UAE Troops," *Middle East Monitor*, March 16, 2018, available at <www.middleeastmonitor.com/20180424-somali-forces-clash-with-uae-troops/>.

[34] Joseph Steigman, "Logistics at the Edge of the Empire: U.S. Army Logistics Trainers in Somalia," *Small Wars Journal*, February 7, 2018, available at <www.hiiraan.com/op4/2018/feb/146795/logistics_at_the_edge_of_the_empire_us_army_logistics_trainers_in_somalia.aspx>.

[35] Ismail Akwei, "Somali Security Forces Turn Against Each Other, 6 Killed in Shootout," *Africa News* (Pointe-Noire, Congo), July 27, 2017, available at <www.africanews.com/2017/07/27/somali-security-forces-turn-against-each-other-6-killed-in-shootout/>; Mohamed Olad Hassan, "At Least Six Killed as Rival Somali Troops Clash in Mogadishu," VOA News, September 16, 2017, available at <www.voanews.com/a/at-least-six-killed-as-rival-somali-troops-clash-in-mogadishu/4031788.html>; "Somalia: NISA, Military Soldiers Clash in the Capital Mogadishu," *Garowe Online* (Puntland, Somalia), October 10, 2017, available at <www.garoweonline.com/en/news/somalia/somalia-nisa-military-soldiers-clash-in-the-capital-mogadishu>.

[36] Jane Ferguson, "Trump's Military Escalation in Somalia Is Spurring Hope and Fear," *The New Yorker*, April 5, 2018, available at <www.newyorker.com/news/news-desk/trumps-military-escalation-in-somalia-is-spurring-hope-and-fear>.

[37] Derek Harvey and Michael Pregent, "Who's to Blame for Iraq Crisis," CNN, June 12, 2014, available at <www.cnn.com/2014/06/12/opinion/pregent-harvey-northern-iraq-collapse/index.html>.

[38] John Beck, "Iraqi Soldiers Fleeing ISIS Claim They Were 'Abandoned' by Senior Officers," VICE News, June 15, 2014, available at <https://news.vice.com/article/iraqi-soldiers-fleeing-isis-claim-they-were-abandoned-by-senior-officers>.

[39] Charles Lister, "One Move Too Far: How Iraq's Nuri al-Maliki Overreached in Anbar," CNN, January 7, 2014, available at <www.cnn.com/2014/01/07/opinion/iraq-anbar-crisis-lister/index.html>.

[40] Zachary Laub, "The Islamic State," Council on Foreign Relations, August 10, 2016, available at <www.cfr.org/backgrounder/islamic-state>.

[41] Mary Grace Lucas, "ISIS Nearly Made It to Baghdad Airport, Top U.S. Military Leader Says," CNN, October 13, 2014, available at <www.cnn.com/2014/10/12/politics/isis-baghdad-martin-dempsey/index.html>.

[42] Ned Parker and Missy Ryan, "Iraqi Military Breakdown Fueled by Corruption, Politics," Reuters, June 13, 2014, available at <www.reuters.com/article/us-iraq-security-military-analysis/iraqi-military-breakdown-fueled-by-corruption-politics-idUSKBN0EO2FK20140614>.

[43] Authors' interview, U.S. military officer, April 13, 2015.

[44] Authors' interviews, Baghdad, Iraq, April 10–16, 2018.

[45] Elise Labott, "5 Questions: What's Going on in Iraq?" CNN, January 6, 2014, available at <https://edition.cnn.com/2014/01/06/politics/iraq-qa/>.

[46] Peter Bergen, "Bergen: It Wasn't Trump but This General's Elite Soldiers Who Defeated ISIS," CNN, December 16, 2017, available at <www.cnn.com/2017/12/15/opinions/it-wasnt-trump-but-this-generals-elite-soldiers-who-defeated-isis-bergen/index.html>.

[47] Renad Mansour, "More Than Militias: Iraq's Popular Mobilization Forces Are Here to Stay," *War on the Rocks*, April 3, 2018, available at <https://warontherocks.com/2018/04/more-than-militias-iraqs-popular-mobilization-forces-are-here-to-stay/>.

[48] Authors' interviews, Baghdad, Iraq, April 10–16, 2018.

[49] William Reno and Jahara Matisek, "A New Era of Insurgent Recruitment: Have 'New' Civil Wars Changed the Dynamic?" *Civil Wars* 20, no. 3 (2018), available at <www.tandfonline.com/doi/full/10.1080/13698249.2018.1497314>.

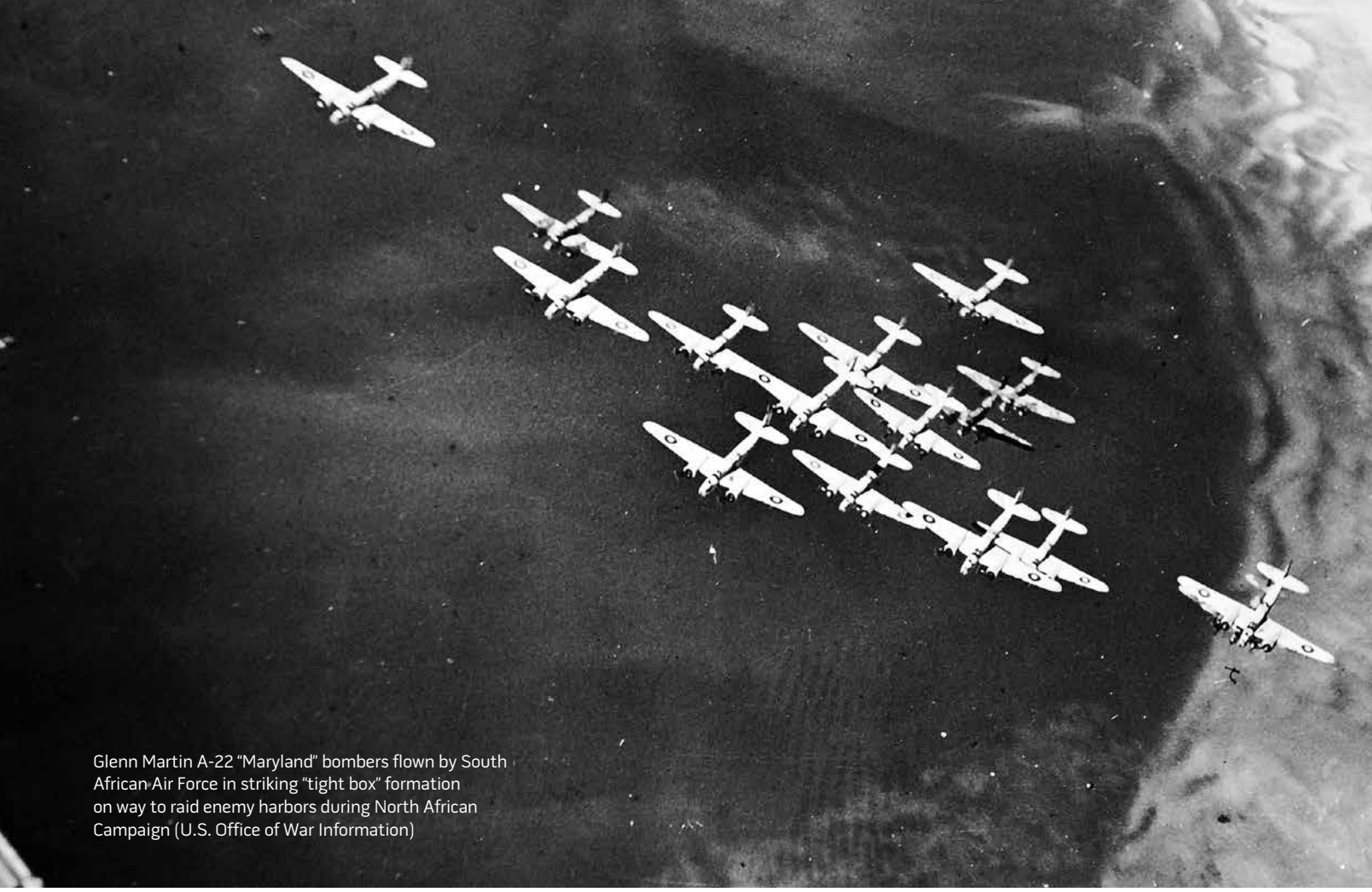
[50] Authors' interviews, American and British personnel, 2017–2018.

[51] Mara E. Karlin, *Building Militaries in Fragile States: Challenges for the United States* (Philadelphia: University of Pennsylvania Press, 2017).

[52] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (New York: Vintage Books, 1964).

[53] Rocky Williams, "Toward the Creation of an African Civil-Military Relations Tradition," *African Journal of Political Science/Revue Africaine de Science Politique* 3, no. 1 (1998), 20–41; Jahara Matisek, "Pathways to Military Effectiveness: Armies and Contemporary African States" (Ph.D. diss., Northwestern University, 2018).

[54] Refer to the Defense Security Cooperation Agency (DSCA) Web site to see its message about the journal being discontinued, available at <www.discs.dsca.mil/_pages/resources/default.aspx?section=publications&type=course_pubs>. In an interview with a DSCA official (April 6, 2017), he lamented the "bad decision" made by a departing DSCA deputy director who saw "no purpose" to the *Defense Institute of Security Assistance Management* [DISAM] *Journal.*



Glenn Martin A-22 "Maryland" bombers flown by South African Air Force in striking "tight box" formation on way to raid enemy harbors during North African Campaign (U.S. Office of War Information)

The Ghosts of Kasserine Pass

Maximizing the Effectiveness of Airpower

By Leland Kinsey Cowie II

Seven decades have passed since combat operations in Tunisia played a seminal role in the evolution of American airpower. In January 1943, the Allied Air Support Command was established in Tunisia to coordinate the efforts of the tactical aircraft assigned to U.S. Army Air Force XII Air Support Command and Number 242 Group Royal Air Force.[1] Upon taking command, Brigadier General Laurence "Larry" Kuter found it to be "a bunch of fighter squadrons and light bombardment squadrons in support of the Second Corps, and [its commander, Major General Lloyd] Friedendahl [sic] had them parceled out here and there, flying umbrellas, and other piece-meal defensive chores."[2] In *Kasserine Pass*, Martin Blumenson illustrates how this marginalized Second Corps' ability to concentrate airpower against an attack by 83 German tanks at the strategic crossroads of Sidi bou Zid on February 14.[3] According to Blumenson, "Except for a flight of four planes that came into the area and left quickly around 10:30, not a single American aircraft would appear all morning despite repeated requests for support."[4] When American ground forces attempted to counterattack the following afternoon, the Allied Air Support Command was unable to stop the unchecked Luftwaffe from conducting three raids.[5] Addressing this "sanguinary American defeat" in *Carl A. Spaatz and the Air War in Europe*, Richard Davis argues that "Allied tactical air did not make its presence felt during the Kasserine engagements until

Lieutenant Colonel Leland Kinsey Cowie II, USAF, is Chief of the Strategy Development Branch, Joint Staff J5.

after the Germans had begun their voluntary withdrawal."[6] Because of this, Allied airmen in North Africa developed new doctrine to achieve success by leveraging unique characteristics inherent to aircraft, now known as the tenets of airpower—centralized control and decentralized execution, flexibility and versatility, synergistic effects, persistence, concentration, priority, and balance.[7]

On October 26, 2016, *The Washington Post* published an article in which Adam Entous and Missy Ryan stated:

The Pentagon has secretly expanded its global network of drone bases to North Africa, deploying unmanned aircraft and U.S. military personnel to a facility in Tunisia to conduct spy missions. . . . The Air Force Reaper drones began flying out of the Tunisian base in late June and have played a key role in an extended U.S. air offensive against an Islamic State stronghold in neighboring Libya.[8]

While technology has pushed contemporary aircraft and weaponry far beyond the capabilities of those employed during World War II, modern doctrine still captures tenets validated by the Tunisian experience in 1943. The authors of Joint Publication 3-30, *Command and Control of Joint Air Operations*, perpetuate these concepts, arguing that "Joint air operations are normally conducted using centralized control and decentralized execution to achieve effective control and foster initiative, responsiveness, and flexibility."[9] As the U.S. Air Force returns to Tunisia, it is appropriate to examine the command relationships and structures used to direct remotely piloted aircraft (RPA) operations to see if they are consistent with the tenets of airpower conceived in North Africa during World War II. Throughout this article, it is evident that the concepts forged in combat over Tunisia 70 years ago stand the test of time; however, to achieve greater efficiencies leveraging the tenets of airpower, the Department of Defense (DOD) must update the doctrine and command structures used to employ networked weapons with global reach.

With a focus on doctrine, the historian and U.S. Air Force Reserve Major General Irving Holley offers a lesson from World War I worth mentioning from *Ideas and Weapons*. According to Holley, "The experience of the war . . . demonstrated that where military authorities failed to formulate a doctrine to exploit each innovation in weapons to the utmost, they suffered disadvantage."[10] This article focuses on four areas to illustrate the ways RPA challenge the current paradigm used to command airpower. First, the article reviews impediments that constrained airpower over Tunisia during the early phases of the North African Campaign. Second, it discusses the role that the Allied experience in North Africa played on the formation of contemporary doctrine. Third, it focuses on current RPA employment and the greater flexibility that networked weapons could offer with a command structure empowered to make dynamic decisions on a global scale. Fourth, it concludes by comparing World War II with contemporary conflicts and makes recommendations for improvement in centralized control and decentralized execution that facilitate the initiative, responsiveness, and flexibility sought by the joint force. Ultimately, doctrine has not evolved to account for the command relationships required to employ networked weapons, such as RPA, in accordance with the tenets of airpower, risking future failures of much greater strategic consequence than those realized at Kasserine Pass.

Airpower in the North African Campaign

Early in World War II, Field Manual (FM) 31-35, *Basic Field Manual: Aviation in Support of Ground Forces* provided the overarching guidance available to the U.S. Army for planning combined air and land operations. At first glance, it appears to perpetuate many of the concepts still resonant in Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations*. For example, the authors of FM 31-35 state, "Flexibility is the ability to concentrate the air effort at short notice on a particular point or distribute it to many points within a relatively short time."[11] Even the assertion that "control is centralized in an air support commander who assigns the attack mission as the needs of the ground unit(s) develop" is similar to the contemporary concept of centralized control and decentralized execution.[12] That said, one of the major differences between FM 31-35 and modern doctrine comes from the declaration that "An air support command is habitually attached to or supports an army in the theater."[13] This provision would significantly constrain the options available to airmen in Tunisia during the runup to Kasserine Pass.

Prior to the Allied invasion of North Africa, the chief-of-staff at Allied Force Headquarters, Brigadier General Walter "Beetle" Smith, issued a series of operational memorandums to provide additional guidance for the Anglo-American forces. On October 13, 1942, Allied Force Headquarters released "Operation Memo No. 17: Combat Aviation in Direct Support of Ground Units." Like FM 31-35, there were parts of the memo intended to increase flexibility. The memo's summary states, "Available direct support aviation must neither be dispersed nor frittered away on unimportant targets. The mass of such support should be reserved for concentration in overwhelming attack upon important objectives."[14] Unfortunately, these principles were incongruent with the command relationship the memo directed: "All air forces of both powers will operate under the command of the Commander-in-Chief, Allied Force. In case the Commander-in-Chief allots a part of the combat aviation to a Task Force, it will operate under the command of the Task Force Commander."[15] The intent of Operation Memo No. 17 was to increase the flexibility of airpower; however, the command relationship it established had the opposite effect.

The command relationships and operational guidance promulgated in FM 31-35 and Operation Memo No. 17 decreased flexibility and reduced the overall effectiveness of airpower in Tunisia. In *Case Studies in the Achievement of Air Superiority*, David Syrett argues that "Most ground commanders in Tunisia

saw aircraft as having essentially two missions: namely to protect ground forces from air attack, which was to be done by maintaining 'air umbrellas' over ground positions, and to act as airborne artillery to attack targets directly in front of the ground forces."[16] On February 5, 1943, Major General Carl "Tooey" Spaatz, Theater Air Commander for the U.S. Army Air Forces, and Kuter met with Fredendall to discuss air support for Second Corps.[17] According to Spaatz, Fredendall "wanted his men to see some bombs dropped on the position immediately in front of them, and if possible, some dive bombers brought down in sight of his troops so that their morale would be bolstered."[18] After wearing out two fighter groups and a light bomber squadron supporting such demands, Syrett claims, "Spaatz told Fredendall 'that if he maintained a constant "umbrella" over one small section of the front with only shallow penetrations by bombers and fighters, that his available force would be dissipated without any lasting effect.'"[19] The command relationships encountered in Tunisia inhibited the flexibility inherent to aircraft.

This point of view was not just isolated to American Airmen or senior officers fighting in North Africa. A Royal Air Force group captain wrote a memo titled, "Some Notes on the Co-Operation Between Ground and Air Forces in Battle," in which he argued:

It is far too often assumed that the only assistance that the air can give to the ground is to provide a fighter cover—or blanket as the Americans call it-over the immediate battle area, and to attack enemy ground forces tactically opposed to our own. With these ideas in his mind, a Military Commander would expect the air forces allocated to assist him to be at his beck and call. . . . It must also be remembered that air power is a mobile weapon and can be transferred from one part of the theater to another under the direction of the Air Commander who has a proper perspective of the whole operation. It is up to him to ensure that his effort is put where it is needed according to the higher requirements, and not dribbled along the front to meet the calls of the local ground commanders.[20]

As the Battle of Kasserine Pass showed, the rigidity observed by this group captain also reduced the Allies' ability to effectively counter Axis actions. The authors of the Royal Army's *History of the Second World War* argue that early in the fight for Tunisia, "Sorties were often carried out in unsuitable weather, and all kinds of targets were accepted without discrimination."[21] Immediate change was needed to overcome the malaise encumbering the employment of Allied airpower. With a clear understanding of the problems confronting airmen early in the North African Campaign, discussion focuses on the doctrine developed to overcome these challenges.

Fortunately, events were unfolding that empowered Allied airmen to improve the efficiency of airpower in Tunisia. At the Casablanca Conference in January 1943, Allied leaders agreed to establish an independent air force chain of command at the theater level, independent of the ground forces.[22] The reorganization, initiated as the Battle of Kasserine Pass was being waged, established the Mediterranean Air Command, under the leadership of Air Chief Marshal Sir Arthur Tedder.[23] Spaatz assumed command of the subordinate Northwest African Air Forces and began instituting organizational changes, including establishing the Northwest African Tactical Air Force from the former Allied Air Support Command.[24] Air Vice Marshal Sir Arthur Coningham took command of the Northwest African Tactical Air Forces, with Kuter staying on as his American Deputy Commander.[25] Frustrated by the ineffective defensive employment of airpower, Kuter stated that Coningham immediately "signed an order prohibiting defensive umbrellas and sent the order to all ground commanders in the area and at higher levels."[26] According to Kuter, Coningham did this so that "there would be no more parceling out of forces, we would go get the enemy."[27]

The revolutionary departure of Coningham's ideas from those outlined in FM 31-35 and Operation Memo No. 17 fostered two spectacular successes in Tunisia. The first was being able to concentrate airpower to shape and counter enemy actions. Kuter recalled that through this ability to focus air operations, "we narrowed the battle area down into the approach to Tunis."[28] After weeks of shaping operations, this ultimately led to a success Kuter described as the "'Great Turkey Shoot,' the time we got the large number of JU-87s"—the same dive bombers that repeatedly attacked American forces during the Battle of Kasserine Pass.[29] Similarly, when an opportunity presented itself, Allied airmen in Tunisia now had the flexibility to take advantage of the situation. On April 10, Spaatz issued the following statement: "The enemy is gradually being forced towards his last strongpoint in NORTHERN TUNISIA. The major responsibility for preventing this withdrawal will fall upon Northwest African Air Forces. There must be no DUNKIRK; the enemy must be ANNIHILATED."[30] The Northwest African Tactical Air Force initiated Operation *Flax* on April 18 to cut Axis lines of communication prior to the start of the Allied ground assault 4 days later.[31]

In what the Germans would come to call *Palmsonntag Massaker* (Palm Sunday Massacre), 112 Axis cargo planes and escort fighters were downed in 48 hours, followed by 20 ME-323 *Gigant* ("Giant") transports carrying a regiment of German reinforcements on April 22.[32] Through the institutional changes implemented in mid-February 1943, Allied airmen in Tunisia were able to, in Kuter's words, "concentrate all the airpower there was at *the* point where it was needed," be it to counter enemy offensive operations or to cut hostile supply lines.[33] The ideas that enabled these spectacular successes were quickly codified as doctrine and became guiding principles for the proper employment of airpower.

Institutionalizing the Lessons from Tunisia as Doctrine

In May 1943, Kuter returned to the Pentagon to serve as the U.S. Army Air Forces Deputy Chief of Staff for Plans and began editing the War Department's FM 100-20, *Command and Employment of Air Power* (1943).[34] Based on his experiences in Tunisia,

Line-up of 13 P-40 "Warhawk" aircraft presented by United States to Fighting French air forces at North African airport, circa 1943 (U.S. Office of War Information)

Kuter confided that he "will take a substantial proportion of the credit for the change in Field Manual 100-20,"[35] specifically, the passage stating:

The inherent flexibility of air power is its greatest asset. Control of available air power must be centralized and command units be exercised through the air force commander if this inherent flexibility and ability to deliver a decisive blow are to be fully exploited. Therefore, the command of air and ground forces in a theater of operation will be vested in the superior commander charged with the actual conduct of operations in the theater, who will exercise command of air forces through the air force commander.[36]

The notion of theater operations guiding the application of airpower, as outlined in FM 100-20, quickly spread throughout the military.

By 1945, the Army Air Forces School of Applied Tactics relied on lessons from Tunisia to form many of the arguments presented in the lesson "The Command and Employment—of—Air Forces."[37] Major Wasson Wilson and Captain Henry Fitzmaurice disparaged previous doctrine, stating that "In giving effect to FM 31-35, specific air units were allocated to the support of corps and divisions. This resulted in loss of the advantage of battle flexibility."[38] Regarding centralized control and decentralized execution, Wilson and Fitzmaurice argue, "The beginning of this conception took place in Tunisia when heavy bombers struck pursuing German tank elements during our withdrawal from the Kasserine Pass on the direction of the theater air force commander."[39] In their view, "The success of the North African operations caused the War Department General Staff to provide in FM 100-20 for functional air forces to be organized along the lines of the Northwest African Air Forces."[40] Air operations in Tunisia, both the failures and successes, serve as the basis for the doctrine still followed by the U.S. Air Force.

The North Africa Campaign is the inspiration behind modern approaches to commanding airpower, be it in academic thought or official doctrine. Proposition eight of Phillip Meilinger's *10 Propositions Regarding Air Power* articulates, "Air Power's unique characteristics necessitate that it be centrally controlled by airmen."[41] In support of this proposition, Meilinger chooses to cite Tedder, the airman entrusted with implementing this principle during North Africa Campaign. Tedder stated, "Air warfare cannot be separated into little packets; it knows no boundaries on land and sea other than those imposed by the radius of action of the aircraft; it is a unity and demands unity of command."[42] Echoing JP 3-30, the authors of Air Force Doctrine Document (AFDD) 1, state, "Because of airpower's unique potential to directly affect the strategic and operational levels of war, it should be controlled by a single Airman who maintains the broad, strategic perspective necessary to balance and

prioritize the use of a powerful, highly desired yet limited force."[43] They go on to state, "Centralized control empowers the air component commander to respond to changes in the operational environment and take advantage of fleeting opportunities."[44] Despite giant leaps in technology since 1943, centralized control still resides at the theater level.

The Unique Characteristics Inherent in RPA

Remotely piloted aircraft provide one example of the "highly desired yet limited force" the authors of AFDD 1 describe.[45] One of the truly revolutionary attributes of RPA is the flexibility fostered by conducting Remote Split Operations (RSO). According to the authors of JP 3-30, "RSO refers to the geographical separation of the launch and recovery crew from the mission crew who employ the aircraft at a location other than where the aircraft is based."[46] In other words, it is a networked system in which the launch and recovery element deploys overseas with the aircraft, while the mission crew element, responsible for piloting the RPA in combat, remains in garrison. As a networked system, it is capable of conducting an RSO shift—the re-tasking of the mission crew element to fly RPA based at different launch and recovery elements. For example, if the weather is bad over Afghanistan, the mission crew element scheduled to pilot those particular aircraft from the United States will conduct an RSO shift and fly RPA from another launch and recovery element, such as the one in Tunisia. The networked nature of RSO has the potential to rapidly increase the flexibility of the high demand yet low density RPA force.

The ability to conduct an RSO shift has provided U.S. Central Command (USCENTCOM) with similar successes as those experienced by the Northwest African Tactical Air Force in Tunisia. Just as Coningham and Kuter were able to concentrate airpower in relation to enemy actions during the Great Turkey Shoot, RPA were able to concentrate against the so-called Islamic State (IS) in June 2014.[47] Within 10 hours of President Barack Obama directing the initiation of operations against IS, an RSO shift from one launch and recovery element to another within USCENTCOM enabled RPA to begin conducting intelligence, surveillance, and reconnaissance (ISR). Another RSO shift is reminiscent of Operation *Flax* cutting the enemy's lines of communication. An RPA mission crew element detected supplies bound for a terrorist organization. Needing additional support to interdict the shipment, USCENTCOM conducted RSO shifts between launch and recovery elements to concentrate airpower over the enemy, resulting in the capture of 46 improvised explosive devices, 213 pounds of C4 plastic explosive, and $995,000 of narcotics. While challenging to coordinate, RSO shifts inside of a single geographic combatant command (GCC) have enabled the flexibility required to concentrate RPA and attain impressive results within the geographic confines of USCENTCOM. Unfortunately, RSO shifts across GCC boundaries are hampered by insufficient authorities, preventing Airmen from globally leveraging the flexibility inherent to RPA. The Air Force must develop the doctrine and command structures required to increase the flexibility of networked weapons both inside and across GCC boundaries.

Despite the capability of the networked RPA force to quickly conduct an RSO shift between distant locations, it still remains a highly desired asset. On September 21, 2016, during a keynote address to the Air Force Association's Air, Space and Cyber Symposium, Chairman of the Joint Chiefs of Staff Joseph Dunford discussed this aspect of the RPA enterprise, stating:

Since 2007, we have increased the numbers of ISR platforms over 600 percent. And today when we sit around with . . . the combatant commanders, we are meeting somewhere less than 30 percent of their ISR requirements. The problem we are confronted with is not how can we afford to buy more Predators. The problem we are confronted with is making decisions, and ensuring that our leadership and our Airmen have the information that they need to make decisions. We'll increase 30 more CAPs [combat air patrols] *. . . that will take us from 60 to 90, and so then we'll be at 34 percent of what the combatant commanders say they need.*[48]

The nature of the problem with the current demand for RPA is not too different from that encountered by Kuter when he took command of the Allied Air Support Command—there are not enough aircraft to provide an adequate air umbrella as determined by the requirements of the supported commanders.

Contemporary RPA and the North Africa Campaign

The difference between World War II and contemporary operations is that networks exceed the scope of the theater-command structure concept established in Tunisia. Realizing that aircraft had the range to rapidly move beyond the area held by a division or corps, command was given to an airman at the geographic-theater level. Now, through RSO shift, RPA have the ability to rapidly engage targets globally, outside a geographic combatant commander's area of operations. The previous examples of RSO shifts all occurred between launch and recovery elements within USCENTCOM. In the Chairman's keynote address, he also characterized the nature of modern threats, stating, "One of the most . . . significant implications . . . is that any future conflict is going to be trans-regional, multi-domain, and multi-functional . . . conflicts are going to quickly spread across combatant command geographic boundaries and domains."[49] Since 2010, IS has conducted simultaneous operations within the confines of three separate geographic combatant commanders: U.S. European Command, U.S. Africa Command, and USCENTCOM.[50] Despite this, DOD does not have a mechanism to prioritize targets and direct weapons in real-time against networked threats spanning GCC boundaries.

Required Doctrinal Changes

Defeating a network requires the ability to attack geographically distant nodes

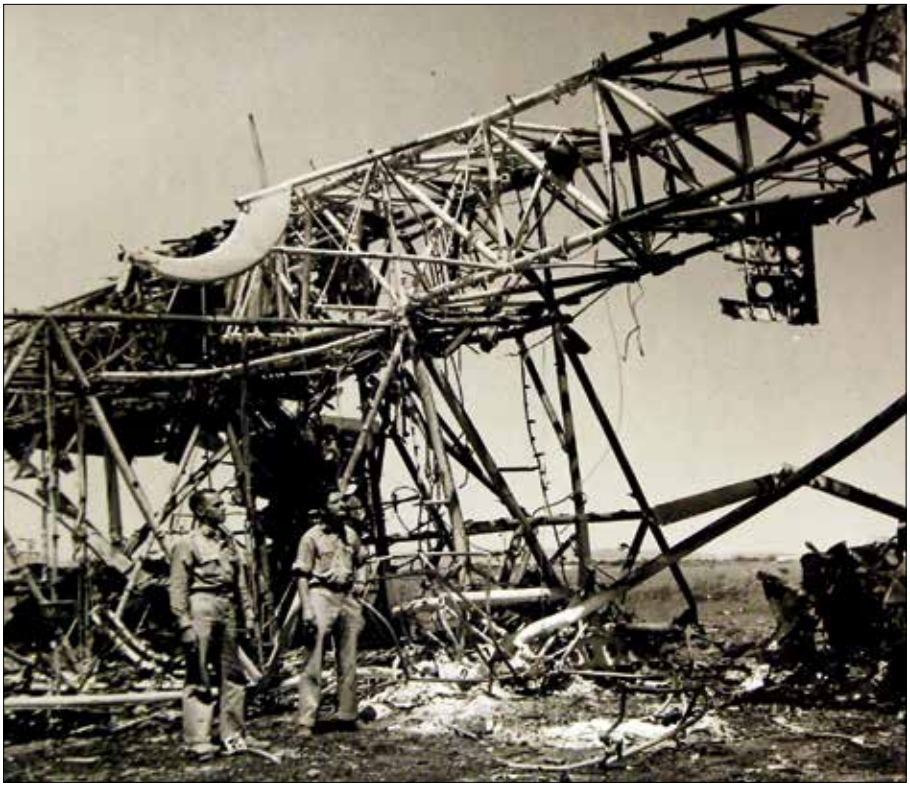
simultaneously, and immediately shift the weight of effort to other distributed emerging or fleeting targets. To borrow an analogy from the military theorist Antoine Bousquet, instead of viewing RPA as an individual tree planted in each theater of operations, it is better to conceptualize the entire enterprise as a rhizome—with a networked root structure spanning GCC boundaries and possessing the ability to shift effort anywhere across the system.[51] Unfortunately, supported commanders tend to measure the contribution of RPA by tallying the number of combat air patrols or "lines" they are allocated, in much the same way that the U.S. Army measured the success of airpower at the Battle of Kasserine Pass by counting the number of Allied aircraft to appear overhead. Networked-RPA operations are still governed by a command structure developed for traditional aircraft, based on theories forged in Tunisia during World War II. There are Service-specific and joint solutions for this problem.

Allied tracer shells tear into early morning sky against raiding enemy aircraft during Operation *Torch*, November 8, 1942 (Library of Congress)

One way to resolve a similar predicament is to employ a Service-specific command structure as first theorized by Kuter. After returning from North Africa, he was responsible for building a plan to field the Boeing B-29 Superfortress—a high-demand yet low-density aircraft. In *Commander in Chief*, Eric Larrabee describes the significance of this weapon, stating, "[the B-29] made up the first aggregate of air power that was truly global, bound to no single theater of operations, . . . in principle they could operate anywhere."[52] According to Kuter, while planning to simultaneously conduct B-29 operations from both the China-Burma-India and Central Pacific theaters, "The idea of parceling out some B-29s to [Admiral Chester] Nimitz and some to [General Douglas] MacArthur where each was so focused on surface Navy and surface Army matters would have been abhorrent."[53] Instead, Kuter designed a command structure that reported to an airman above the theater level—the Twentieth Air Force, commanded by General Henry "Hap" Arnold.[54] Also Chief of the Army Air Forces, Arnold ensured that B-29 operations were consistent with the strategic guidance issued by the Joint and Combined Chiefs.[55] While the military departments lost the ability to execute operations in 1958, and the Goldwater-Nichols Defense Reorganization Act of 1986 established an unambiguous chain of command linking the President, Secretary of Defense, and the combatant commanders, emerging technologies may dictate the revival of Service control over certain weapons.[56] Be it low-density RPA, space, or cyber weapons, if authorized, the Air Force could appoint an officer to serve as a global joint force air component commander to prioritize and allocate networked airpower in real time. This would be similar to the role fulfilled by the commander of Air Mobility Command and executed through the 618th Air Operations Center, the Tanker Airlift Control Center, in supporting the mission of U.S. Transportation Command.[57]

Joint solutions could provide another option for commanding networked weapons. The organization designed to command B-29 operations matured to account for other advances in strategic weapons, including intercontinental and submarine-launched ballistic missiles, first as the Strategic Air Command and later as U.S. Strategic Command. A functional component, such as U.S. Strategic Command, could command globally networked weapons. There is also the potential to get approval for an officer serving in the Joint Chiefs of Staff Operations Directorate to fulfill this role—similar to Arnold, but without building an associated Service-specific command structure.

Similarly, the National Reconnaissance Office operates the satellite constellation responsible for intelligence collection. Based on the judgment of the National Reconnaissance Office and in keeping with established intelligence priorities, the satellites are continuously re-tasked to various targets both inside and across GCC boundaries. The authors of JP 3-52, *Joint Airspace Control*, suggest the use of procedural control measures, similar to the coordination level used to separate helicopters from fixed-wing planes, to separate RPA from traditional aircraft.[58] Under this model, the RPA would be centrally controlled and launched as tasked using the



Axis air equipment and installations took heavy pounding from bombers of U.S. Army Air Forces during Battle of Tunisia, November 1942 to May 1943 (U.S. Army Air Forces/Library of Congress/Nick Parrino)

procedural-airspace control measures that allow for the conduct of operations at any time in each GCC. The RPA would still appear on the Air Tasking Order and be available to the geographic combatant commander to conduct strike operations when necessary; however, the centralized manager of their intelligence missions would have the authority to conduct RSO shifts in accordance with global priorities. In essence, RPA would be treated like satellites and operate freely within a GCC, with the exception that they fly within the atmosphere and require procedural airspace control measures to avoid being a conflict to other aircraft. The success of any option requires combatant commanders to stop counting the number of RPA "lines" their theater receives and instead focus on the effects the weapons provide.

Conclusion

Whatever the solution, combatant commanders must be willing to support the decisions of the officer appointed to command networked weapons—as their individual operations will at times be either enhanced or hindered by such judgments.[59] Regarding RPA, it is important to note that an RSO shift is of temporary nature, as it forces the gaining launch and recovery element to surge its equipment and personnel. To date, RPA operations are coordinated through an Air Force wing operations center; however, it does not have the authority to direct an RSO shift either inside or across GCC boundaries as a result of emerging strategic opportunities. Ultimately, as General Dunford recently wrote in *Joint Force Quarterly*, "Our decisionmaking processes and planning constructs must . . . be flexible enough to deliver options at the speed of war."[60] In order for networked weapons, such as RPA, to overcome bureaucracy and keep pace with the speed of war, they must be commanded by an *Airman* with the authority to reallocate them across administrative-geographic boundaries in real time.

The authors of AFDD 1 emphasize that "Any doctrine document is a snapshot in time—a reflection of the thinking at the time of its creation. Doctrine should evolve as new experiences and advances in technology point the way to the operations of the future."[61] During World War II, Tunisia illustrated the consequences of allowing technological development to outpace doctrine and military thought. Collectively, Tedder, Spaatz, Coningham, and Kuter built a system that centralized the control of airpower under the command of airmen, allowing aircraft to leverage the tenets of airpower and shape the battlespace out to the limits of their operational range.

In the 21st century, RPA can hold any target at risk within range of the global network. As the Air Force returns to Tunisia, it is important to apply the lessons forged in hostile skies over 70 years ago. First, just as the B-29 foreshadowed other future strategic weapons, the RPA is a harbinger of things to come. Any viable long-term solution to the problems associated with commanding networked weapons must be platform agnostic. Second, the officer entrusted to command these weapons must be empowered to make real-time decisions regarding employment across the entire breadth of the network, in accordance with the tenets of airpower. Third, command of RPA must reside with an *Airman*, subordinating these assets to geographic combatant commanders is no different than condoning modern-day air umbrellas. The principles developed in North Africa stand as true today as they did in 1943; however, doctrine must support command relationships that maximize the efficiency of modern-networked weapons for the joint force. The words the Chairman chose to close his article for *JFQ* are equally as fitting for this study, "The character of war in the 21st century has changed, and if we fail to keep pace with the speed of war, we will lose the ability to compete."[62] **JFQ**

Notes

[1] Major-General I.S.O. Playfair et al., *The Mediterranean and Middle East*, vol. 4: *The Destruction of the Axis Forces in Africa*, in *History of the Second World War*, ed. Sir James Butler (London: Her Majesty's Stationery Office, 1966), 311.

[2] Laurence S. Kuter, "Night Bombing in the Battle Area," January 24, 1943, IRIS Number 24998 (Maxwell Air Force Base [AFB], Air Force Historical Research Agency [AFHRA]); Laurence S. Kuter, interview by Tom Sturm and Hugh Ahmann, September 30–October 3, 1974, Naples, FL, USAF Oral History Program (Maxwell AFB: Albert F. Simpson Historical Research Center), 283.

[3] Martin Blumenson, *Kasserine Pass* (Boston: Houghton Mifflin Company, 1967), 143.

[4] Ibid., 142.

[5] George F. Howe, *Northwest Africa: Seizing the Initiative in the West* of *United States Army in World War II: The Mediterranean Theater of Operations* (Washington, DC: Government Printing Office [GPO], 1957), 420.

[6] Richard G. Davis, *Carl A. Spaatz and the Air War in Europe* (Washington, DC: GPO, 1993), 178, 183.

[7] Air Force Doctrine Document (AFDD) 1, *Basic Doctrine, Organization, and Command* (Washington, DC: Headquarters Department of the Air Force, October 14, 2011), 37.

[8] Adam Entous and Missy Ryan, "U.S. Has Secretly Expanded Its Global Network of Drone Bases to North Africa," *Washington Post*, October 26, 2016, available at <www.washingtonpost.com/world/national-security/us-has-secretly-expanded-its-global-network-of-drone-bases-to-north-africa/2016/10/26/ff19633c-9b7d-11e6-9980-50913d68eacb_story.html?utm_term=.4bd9e9f921a1>.

[9] Joint Publication (JP) 3-30, *Command and Control of Air Operations* (Washington, DC: The Joint Staff, February 10, 2014), ix, available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf>.

[10] Irving Brinton Holley, Jr., *Ideas and Weapons* (Washington, DC: GPO, 1997), 176.

[11] Field Manual (FM) 31-35, *Basic Field Manual: Aviation in Support of Ground Forces* (Washington, DC: War Department, April 9, 1942), 6, available at <http://cdm16040.contentdm.oclc.org/cdm/ref/collection/p4013coll9/id/932>.

[12] Ibid., 3.

[13] Ibid., 1.

[14] Walter Bedell Smith, Allied Force Headquarters, "Operation Memo No. 17: Combat Aviation in Direct Support of Ground Units," October 13, 1942, IRIS Number 233080 (Maxwell AFB: AFHRA), 5.

[15] Ibid., 1.

[16] David Syrett, "Northwest Africa, 1942–1943," in *Case Studies in the Achievement of Air Superiority*, ed. Benjamin F. Cooling (Washington, DC: GPO, 1994), 242.

[17] Ibid., 241.

[18] Ibid.

[19] Ibid.

[20] Group Captain, "Some Notes on the Co-Operation Between Ground and Air Forces in Battle," March 17, 1943, IRIS Number 24998 (Maxwell AFB: AFHRA). The group captain's signature is illegible and his signature block only contained his rank and Service.

[21] Playfair et al., *The Mediterranean and Middle East*, vol. 4, 310.

[22] Davis, *Carl A. Spaatz and the Air War in Europe*, 180 and 183.

[23] Carl Spaatz, "General Orders Number 1," February 18, 1943, IRIS Number 2002141 (Maxwell AFB: AFHRA).

[24] Ibid.

[25] Air Historical Group, *The Army Air Forces in World War II*, vol. 2: *Europe: Torch to Pointblank: August 1942 to December 1943*, ed. Wesley Frank Craven and James Lea Cate (Chicago: The University of Chicago Press, 1949), 157.

[26] Laurence S. Kuter, MS 18, addendum 1, box 4, folder 1, Laurence S. Kuter Papers, Gimbel Aeronautical History Collection, Robert F. McDermott Library, USAF Academy, CO.

[27] Kuter, interview by Sturm and Ahmann, 293.

[28] Ibid., 308.

[29] Ibid.

[30] Carl Spaatz, "Memorandum," April 10, 1943, IRIS Number 24998 (Maxwell AFB: AFHRA).

[31] "Statement by Brigadier General Laurence S. Kuter at Press Conference in the Pentagon, May 22, 1943," IRIS Number 242513 (Maxwell AFB: AFHRA), 5.

[32] Ibid., 6.

[33] Kuter, interview by Sturm and Ahmann, 315. Emphasis in original.

[34] Ethel Kuter, MS 18, addendum 1, box 4, folder 4, Laurence S. Kuter Papers, Gimbel Aeronautical History Collection, Robert F. McDermott Library, USAF Academy, CO.

[35] Ibid.

[36] Ibid.

[37] Wasson J. Wilson and Henry F. Fitzmaurice, "Command and Employment—of—Air Forces," January 10, 1945, Roll A2840 (Maxwell AFB: AFHRA).

[38] Ibid., 11.

[39] Ibid., 16.

[40] Ibid., 14.

[41] Phillip S. Meilinger, *10 Propositions Regarding Air Power* (Maxwell AFB: School of Advanced Airpower Studies, Air University, 1995), 49.

[42] Ibid.

[43] AFDD 1, 38. The passage is in bold print in the original source.

[44] Ibid. The passage is in bold print in the original source.

[45] Ibid.

[46] JP 3-30, *Command and Control of Air Operations*, III-31.

[47] While unclassified, the information contained in this section came from two sources that are not publicly verifiable. Some information was taken from an Air Force Form 707, "Officer Performance Report (Lt thru Col)," for a remotely piloted aircraft (RPA) squadron's director of operations. The remaining information came from an Air Force Form 1206, "Nomination for Award," used to submit an RPA squadron for an annual Air Force–level award.

[48] Joseph F. Dunford, Jr., "2016 Air Force Association's Air, Space and Cyber Conference: CJCS Joe Dunford Keynote Address," video, 47.03, Washington, DC, September 21, 2016, available at <www.youtube.com/watch?v=9_mLtv1iNF4>.

[49] Ibid.

[50] Entous and Ryan, "U.S. Has Secretly Expanded Its Global Network of Drone Bases to North Africa."

[51] Antoine Bousquet, "Chaoplexic Warfare," lecture to the Air War College Grand Strategy Program via Skype from the United Kingdom, Maxwell AFB, January 11, 2017.

[52] Eric Larrabee, *Commander in Chief: Franklin Delano Roosevelt, his Lieutenants, and their War* (New York: Harper & Row, 1987), 580.

[53] Kuter, interview by Sturm and Ahmann, 388.

[54] Ibid., 278.

[55] Larrabee, *Commander in Chief*, 580.

[56] James R. Locher III, *Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon* (College Station: Texas A&M University Press, 2002), 440.

[57] JP 3-30, *Command and Control of Air Operations*, III-29.

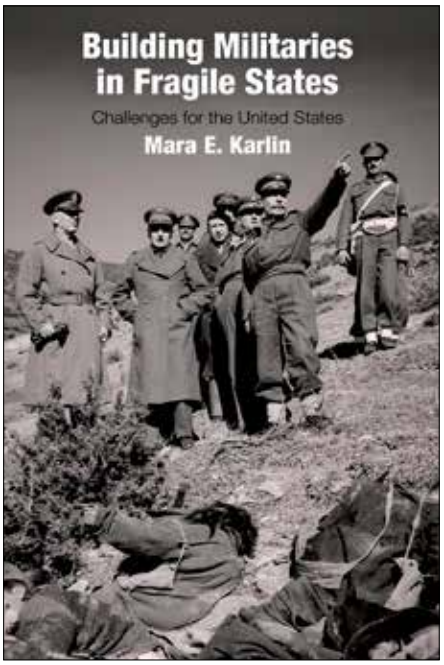
[58] JP 3-52, *Joint Airspace Control* (Washington, DC: The Joint Staff, November 13, 2014), III-10, available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_52.pdf>.

[59] On page II-2 of JP 3-30, *Command and Control of Air Operations*, the authors state, "The JFC [joint force commander] will normally assign JFACC [joint force air component commander] responsibilities to the component commander having the preponderance of forces to be tasked and the ability to effectively plan, task, and control joint air operations." To borrow from the ideas presented by JP 3-30, in the future it will be important that the designated commander for networked weapons have the preponderance of forces to be tasked and the ability to effectively plan, task, and control joint networked weapons operations. With this argument's focus on airpower, the term *Airman* is used to denote the commander most likely to be designated with this responsibility for RPA. As more networked weapons are fielded, the appointed commander must be the candidate most capable of achieving strategic advantage through their employment—which may, or may not, necessarily be an Airman.

[60] Joseph F. Dunford, Jr., "The Pace of Change," *Joint Force Quarterly* 84 (1st Quarter 2017), 3, available at <https://ndupress.ndu.edu/Media/News/Article/1038776/from-the-chairman/>.

[61] AFDD 1, 7.

[62] Dunford, "The Pace of Change," 3.



Building Militaries in Fragile States: Challenges for the United States

By Mara E. Karlin
University of Pennsylvania Press, 2017
$75.00 296 pp.
ISBN: 978-0812249262

Reviewed by John L. Hewitt III

Have you ever wondered why the United States has such an "uneven" record when it comes to building foreign militaries? Since the United States has been involved in building militaries since World War II, one would think it would be adept at doing this, particularly considering its military funding, training, and equipping apparatus. However, this is not the case, as illustrated by measured, objective studies.

Mara Karlin, former Pentagon policymaker and current associate professor of practice of strategic studies at The Johns Hopkins University, has taken a serious look at the nuts and bolts of building militaries abroad—why strategies do and do not work—and the results of U.S. attempts to build militaries in fragile states.

In *Building Militaries in Fragile States*, Karlin provides a thoughtful, well-researched, and comprehensive account of the components of and challenges associated with U.S. attempts to build militaries through four case studies: Greece (1947), South Vietnam (1955), Lebanon (1982), and Lebanon (2005). As she notes, according to former Secretary of Defense Robert Gates, security cooperation or building militaries "is one of the serious security challenges of our times" and must be addressed appropriately. Karlin further asserts, "It can be done cheaply and potentially reduce casualties," which the U.S. populace would undoubtedly support. Moreover, "building partner militaries will likely be increasingly seen as an easier and cheaper way to handle them" in the future.

Karlin states that it is not more training, equipping, and funding that are needed. These things do not address a foreign military's key requirement, which is, Karlin concludes, "to exert the government's sovereignty throughout its territory." Instead, she contends, the United States must be "deeply involved in the partner state's sensitive military affairs, not operating on the periphery (or passively), and ensure that antagonistic external actors play a diminishing role, instead of degrading the gains brought about by U.S. involvement." This is important as it determines whether "the partner state military is likely to establish an internal defense."

Karlin's book includes much useful data, via charts, tables, and other graphical aids, and is bolstered by personal accounts from leaders, decisionmakers, diplomats, general officers (both U.S. and foreign), Department of Defense (DOD) officials, and others who are charged with structuring or restructuring, funding, equipping, training, and leading efforts to build nascent or immature militaries. Best of all, Karlin offers a glimpse behind the secretive curtains of the Oval Office (Presidents Harry Truman, Dwight D. Eisenhower, Ronald Reagan, George W. Bush, and Barack Obama), DOD and Department of State, U.S. Embassies, and the National Security Council, where readers become privy to somber, prudent, and reflective accounts regarding the complexities and challenges of these missions.

Karlin introduces readers to a volatile mix of dynamics including frail and stout egos, domineering and acquiescing personalities, strong and fragile leadership, Presidential entreaties (and blunders), wavering and staunch commitments, intra- and inter-departmental infighting and cohesion, and discordant approaches and points of view toward mission strategy and implementation. The dynamics manifest themselves throughout the study and generally yield predictable results—success or failure. In Greece, for example, the U.S. "involvement in military affairs was deep, the U.S. did not become co-combatants, and it managed to reduce the impact external actors had on Greece." In Vietnam, U.S. involvement in military affairs was "limited, and it overreacted to concerns to external actors." The case was similar in Lebanon (1982 and 2005), where external aggression in the form of Syria, Iran, and Israel, and internal aggressors like Hezbollah induced considerable pressure on Lebanon and the United States, requiring the two sides to essentially agree to disagree on the appropriate strategy.

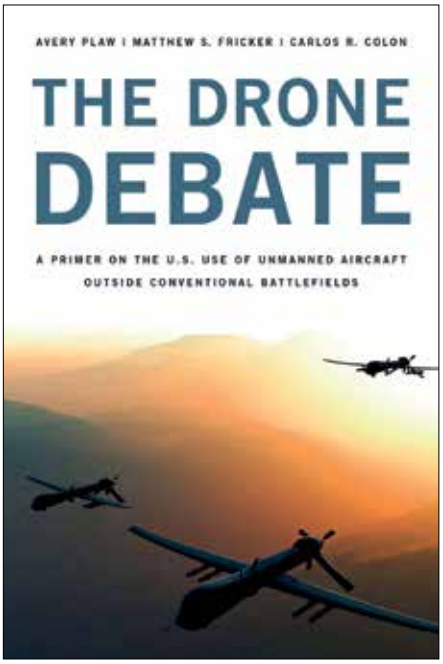
Karlin closes the book with a thought-provoking chapter devoted to recommendations. She succinctly recaps the cases, identifying where the host nation and the United States succeeded or failed. Her bold prescriptions for policymakers to consider in future endeavors are helpful. The author herself admits the book's lone limitation, with respect to the relatively small number of countries analyzed, acknowledging that "this book laid the groundwork for future research on strengthening partner militaries for internal defense."

To be clear, the book is not a school solution or completed answer sheet to the test. Instead, it serves as a playbook for policymakers to analyze and deduce historical problems, juxtapose those against today's challenges, reconcile them, and then identify mechanisms that contribute successfully to building militaries.

Building Militaries in Fragile States is a formidable contribution to this field of study; it is prescriptive, detailed, and informative. The author provides readers a roadmap for further investigation that

should elicit robust conversations, deeper analysis, and decisive actions. I recommend this book to foreign policy analysts, policy wonks, military personnel, and anyone interested in foreign affairs. Mara Karlin illuminates a problem that will no doubt bedevil the United States for decades—her insights are both enlightening and frightening. **JFQ**

John L. Hewitt III is the Command Executive Officer of the 86th Training Division, Fort McCoy, Wisconsin.



The Drone Debate: A Primer on the U.S. Use of Unmanned Aircraft Outside of Conventional Battlefields

By Avery Plaw, Matthew S. Fricker, and Carlos R. Colon
Rowman & Littlefield, 2015
$38.00 354 pp.
ISBN: 978-1442230590

Reviewed by Matthew Mueller

Since the first use of a drone strike outside a conventional battlefield in November 2002, the United States is credibly reported to have carried out at least 500 covert strikes in Pakistan, Yemen, and Somalia, killing around 3,500 people, including civilians. Indeed, drones became the poster child for U.S. counterterrorism operations under the administration of President Barack Obama and have generated growing attention and controversy. The authors of this book sought to develop a primer that summarized the debate on several key issues related to drones. It is important to note, as the authors do at the outset, that this book focuses only on the use of drones *outside* of conventional battlefields and for this reason excludes operations conducted by the United States in countries like Afghanistan and Iraq. While *The Drone Debate* covers a wide range of material, it does so with exceptional clarity and objective analysis that allow readers to come to their own conclusions surrounding the important questions drones raise.

The book proceeds through the different dimensions of the debate, beginning with a concise overview of the history of drone operations. This sets up the rest of the book by providing readers with the historical development of drones since the end of World War II until today, as well as an understanding of the different open-source databases that catalog drone strike casualties. Regardless of which database is being considered, the evidence shows that as drone technology has evolved, civilian casualties have decreased, suggesting that their use is becoming more discriminating due to better technology and/or stricter targeting guidelines. The authors' careful attention given to explaining the differences among the four main open-source drone strike casualty databases (New America, The Bureau of Investigative Journalism, Long War Journal, and the Center for the Study of Targeted Killing) is commendable. While similar, each database uses its own coding that produces different results; the authors have provided readers an easily digestible explanation of the differences. Picking up from this, the authors conduct an exceptional tour de force through the strategic, legal, ethical, and political issues surrounding the use of drones in Pakistan, Yemen, and Somalia.

The authors also provide a good presentation of the debate surrounding the efficacy of drone strikes by looking at issues surrounding their precision and whether drone strikes are indeed an effective strategy for combating terrorism. Many critics have asserted that the use of drone strikes has had a paradoxical effect on al Qaeda; while these strikes have succeeded in removing mid- to senior-level leaders, they have also opened the opportunity for younger, more radical leaders to take their places. The occurrence of civilian casualties has only invigorated al Qaeda's recruitment efforts. In response, defenders of the drone program have argued that the number of civilian casualties is inflated and that the operational and psychological impact of drone strikes on al Qaeda leadership has had a significantly disruptive effect on the group's operations. The authors conclude that, while there are many forceful arguments on both sides, there is not a single knockout argument for either.

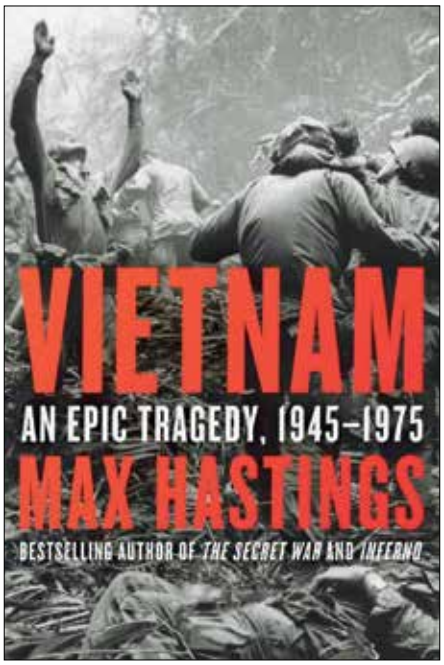
The legality and ethics of using drones outside of conventional battlefields are hotly debated. The authors sketch an overview of the legal issues present under both U.S. domestic law and international law. The third chapter is admittedly a slightly difficult chapter to read due to the debate surrounding the conflict classification between the United States and al Qaeda and affiliated forces. The authors do their best to walk through the application of the international law of self-defense and international humanitarian law, but the lurking issue of what type of conflict (international armed conflict, noninternational armed conflict, or—as some in the literature base on conflict classification have argued—transnational armed conflict) is at hand is evident in any discussion of the legality of drones strikes under international law. In contrast, the fourth chapter provides an excellent overview of the different ethical issues surrounding drones, including the application of Just War Theory, the effect on military virtues, the question of whether drones will increase the propensity for armed conflict, and the ethics of the use of fully autonomous weapon systems.

The discussion on political implications is thought to be self-explanatory: there is a fairly firm domestic political base in the United States for using drones to strike suspected terrorists abroad. While aggregate data generally show the majority of Americans support the use of drone strikes against suspected terrorists, the authors' presentation of opinion data for specific segments of the population presents a more nuanced picture. The poll data presented in the case study show that support in the United States is not as robust as advocates claim. The inclusion of case studies in each chapter that offer deeper dives into aspects of the debate surrounding drones is one of the book's fundamental strengths. The chapters themselves cover all of the key points, and the case studies allow the chapters to engage with the most important issues in greater depth.

The final chapter is the most interesting. Addressing the emerging issue of drone proliferation, the authors walk through the differing thoughts on the effects that diffusion of drone technology will have. They examine the unconfirmed use of a drone by Hizballah on September 21, 2014, to target al-Nusra Front fighters in Syria. This raises the question as to what happens when states lose the monopoly of this technology.

By highlighting the key arguments on both sides of the debate about drones, the authors present each side as equally as possible. The book touches on the right issues; however, those who are looking for fresh arguments regarding drones should look elsewhere. The authors' balance and breadth make this book ideal for classroom use. While the book does not offer anything original to the growing literature on drone use, it does serve as an effective teaching tool for those seeking to learn about the issues surrounding drone use outside conventional battlefields. **JFQ**

Matthew Mueller wrote this review as a graduate student in the School of International Relations at the University of St. Andrews in Scotland. He now works at the Institute for the Study of War.



Vietnam: An Epic Tragedy, 1945–1975

By Max Hastings
Harper Collins, 2018
$37.50 896 pp.
ISBN: 978-0062405661

Reviewed by Williamson Murray

Max Hastings has had a spectacular career as a historian, journalist, and newspaper editor. He has now turned his attention to writing a history of the Vietnam War, from its inception with French colonial rule to the final denouement in spring 1975. The word *tragic* is all too often overused, but in this case, Hastings is correct to term the tale that he covers a long and epic tragedy. As with so many of his other books, he discusses with penetrating insight the arrogance and abysmal political and military leadership of the war at the highest levels. But in the end, it was those soldiers and civilians at the lowest levels who suffered the most from the mistakes, faulty assumptions, and carelessness of their supposed betters.

What makes Hastings such an extraordinary historian is the fact that he brings his journalist sense to sniff out the stories and performance of those who participated in discussions and decisionmaking at the highest levels. This quality also makes him a wonderful interviewer of the living, whether they are political leaders, military leaders, or common soldiers. It also provides him the ability to bring to life the dry political and military records of the past as well as the oral interviews that the American military conducted during and after the war. Moreover, Hastings, having covered political and military leaders over the past five decades, has a real sense of what drives them. For the most part, the leadership of the French, Americans, and Vietnamese—southern as well as northern—was worse than abysmal; they made a troubled and difficult situation much worse that it ought to have been.

On the French side, military leaders started the war with an unjustified contempt for the Vietnamese. The army they brought to Southeast Asia consisted of professional French soldiers, the hodgepodge of nationalities who make up the French Foreign Legion, and colonial troops drawn from Algeria, Morocco, and francophone Africa. None had the slightest interest in providing an alternative to the Viet Minh under Ho Chi Minh and his supposedly amateur general Vo Nguyen Giap, who appears as one of the few senior military leaders who possessed a realistic sense of the political and military equations in the war. The sorry French effort eventually collapsed at Dien Bien Phu in spring 1954, when French generals committed some of their best troops to a hopeless fight and then spent the months of March, April, and May quarreling among themselves and begging the Americans for aid as their troops died. On the other side, Giap provided generalship that was both sophisticated and ruthless.

As a result, the French abandoned their colonies in Indochina (Vietnam, Laos, and Cambodia) in 1954, while the Americans thought they had saved at least a portion of Vietnam from communist evils with the Geneva Peace Accords. In fact, they had not saved anything—they only prolonged the agony for the Vietnamese and eventually a

sizeable number of Americans. But it was the Vietnamese who suffered the most in the aftermath of the war to drive the French out. Those in the north suffered under a merciless and fanatical communist dictatorship that aimed to impose the nirvana promised by Karl Marx on a desperately poor population, those in the south under an incompetent regime run by corrupt generals, and eventually Americans who understood virtually nothing about Vietnamese history, culture, and language. In effect, the Viet Minh victory at Dien Bien Phu had made the survival of South Vietnam, even under competent leadership, virtually impossible, and the South Vietnamese received anything but that.

From 1955 on, the Americans provided mountains of cash, weapons, and ammunition, but few of those dealing with South Vietnam possessed either any sense of the political and military difficulties involved in fighting an insurgency or the complexities of the human environment that was South Vietnam. Unfortunately for all concerned, the American performance was marked by extraordinary arrogance and contempt for those who knew something about the area. Among the worst were Lyndon Johnson and Robert McNamara, who enthusiastically lied to the American people, deployed military forces as a means of sending signals, and remained consistently ignorant of the nature of North Vietnamese leaders. Above all, neither they nor their generals developed a clear strategy or rationale for committing tens of thousands and then hundreds of thousands of young Americans to a war that made no strategic sense. McNamara clearly deserves his reputation as the Secretary of Defense who managed to do the most damage to the United States, which he was supposed to protect. For their part, President Richard Nixon and Henry Kissinger reached a level of cynicism that is truly astonishing, and their efforts to preserve American honor during their tenure in office failed completely at a cost of more than 15,000 Americans dead and untold numbers of Vietnamese casualties. All this Hastings records with a sharpness and clear understanding of the ability of those in power to misuse their positions.

The performance of the American generals was dismal. Unimaginative and misunderstanding the nature of the war, General William Westmoreland, commander of Military Assistance Command, Vietnam, developed a firepower-intensive war that smashed up the landscape, killed far more civilians than the Viet Cong, and paid little attention to the political framework within which the war was being fought. He was also the worst kind of "looking good general." On the first night of the Tet Offensive, when the 716th Military Police Battalion, the only U.S. Army unit in Saigon's center, refused to come to the aid of the Embassy under attack, Westmoreland remained ensconced in his quarters for 5 hours until just after American paratroopers had secured the Embassy.

Westmoreland then chewed out the paratrooper captain and his men, who had been fighting over the past several hours to kill the Viet Cong sappers, for their appearance and ordered them to smarten up. To another American, "the general expressed disgust at the unseemly mess. 'I suggest you get this place cleaned up,' he told the duty officer, 'and get these people back to work by noon.'" As for the political repercussions of the attack on the Embassy, Westmoreland did not have a clue. But the most significant mistake the general was to make during the Tet Offensive and the American and South Vietnamese counteroffensive was to focus on Khe Sanh, while the Viet Cong were slaughtering the population in Hue and other cities. It was the vicious battle for Hue, the ancient capital of Vietnam, that probably did the most damage to American attitudes back home.

But as Hastings underlines throughout his account, the other side of the hill had as its leaders a group of truly ruthless, murderous ideologues. For those who have not followed the revelations that have been coming out over the past decade from Hanoi, Hastings's account of the North Vietnamese leadership will be eye-opening. By the early 1960s, Ho Chi Minh and Giap had been largely removed from political and military decisionmaking. The crucial political decisions were now in the hands of Le Duan and Le Duc Tho, two ferociously committed Stalinists, who would consistently get the war in the south wrong. But in the highly charged political atmosphere of North Vietnam, ideological commitment was everything and the reality of American strength was a mere bagatelle. Thus in 1964, during the Tonkin Gulf Crisis, Le Duan had contemptuously dismissed Giap's worry about getting involved with the Americans with the comment that "He's as timid as a rabbit."

Not surprisingly, Le Duan was behind the Tet Offensive of January 1968 in spite of Giap's warnings about American firepower and his belief that the Americans would withdraw in the near future. The former clearly believed that the result of such an offensive would lead to a popular revolt that would drive the Americans out and overthrow the "puppet" regime: "If you wanted victory, guerrilla struggle had to evolve into large-scale conventional war. Half a million people will take up arms for us." Again, events proved him wrong. Tet, exceedingly badly planned so that attacks occurred with minimal reconnaissance, and in most areas badly executed by the attackers, whether North Vietnamese or Viet Cong, resulted in a disastrous military defeat, especially for the latter.

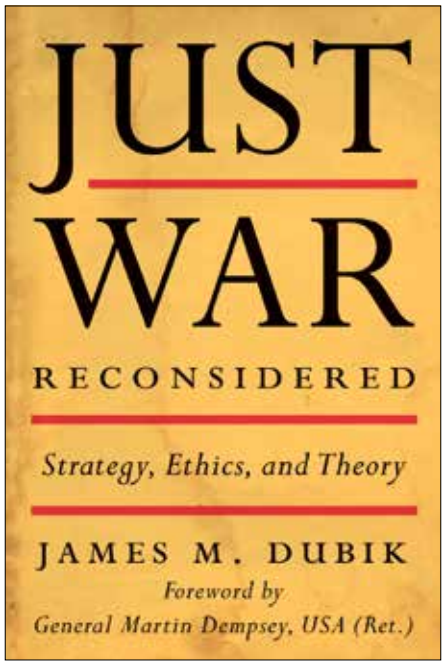
Nevertheless, the dismal military results had little impact on Le Duan's control over the regime and its army. As one Viet Cong observer of his brethren in the north commented, "they had sacrificed conscience and pragmatism for the certitudes of their political religion. Amid their steely arrogance, there was no latitude for compromise." Learning nothing from his past mistakes, Le Duan was the author of the spring 1972 Easter Offensive that again proved a military disaster. He remained in power, although Giap would return to run the 1975 offensive that finally crushed South Vietnam.

Caught between the implacable, ferocious North Vietnamese and Viet Cong communists on one side, and the Americans with their indiscriminate use

of firepower, the Vietnamese people, north and south, suffered unimaginable trials. What makes *Vietnam* such an impressive study is Hastings's ability to weave the stories of common soldiers and civilians on both sides of the struggle into a terrifying and impressive tale of both man's inhumanity to his fellows, and the heroism of those on the sharp end. He is able, thus, to connect the highest levels of decisionmaking in Hanoi, Washington, and Saigon, while at the same time providing the reader with a sense of the terrible consequences that often result from those who make the decisions with little understanding or concern for their impact on those below them.

From the American point of view, perhaps the saddest result of U.S. participation in this conflict was that U.S. political and military leaders and their people learned so little from the price they paid for our participation in the war. JFQ

Dr. Williamson Murray is Professor Emeritus at The Ohio State University. He has taught at the U.S. Army War College, U.S. Naval War College, U.S. Naval Academy, and Marine Corps University.



Just War Reconsidered: Strategy, Ethics, and Theory

By James Dubik
University of Kentucky Press, 2016
$25.00 236 pp.
ISBN: 978-0813175010

Reviewed by C. Anthony Pfaff

Lieutenant General James Dubik, USA (Ret.), in his *Just War Reconsidered*, provides a provocative account of perhaps Just War Theory's greatest blind spot: accountability of senior political and military leaders for the decisions they make regarding how to wage war. Traditionally, Just War theories divide decisions about war into two broad categories: *jus ad bellum*, which are the right reasons to go to war, and *jus in bello*, which governs right conduct in war. This account only holds the civilian leadership accountable for the decision to go to war, and the military leadership accountable for how they treat enemy combatants and noncombatants when fighting the war. It excludes from governance what either set of leaders does to its own troops or peoples.

Dubik argues that there must be principles that guide senior leaders' conduct in the waging of war, which he defines as achieving coherence by setting war aims and aligning strategy and policy to achieve those aims; generating organizational capacity to achieve those aims at the least cost in terms of lives and resources; and maintaining legitimacy of the war effort by observing the war convention, sustaining public support, and ensuring proper subordination of the military-to-civilian leadership. As he states, "Poor war aims, strategies, and policies, badly thought-through campaigns and major operations, and inefficient and ineffective civil-military dialogue and execution" can prolong war unnecessarily, wasting precious national resources and, more importantly, lives, while placing the political community at risk. So by leaving war-waging out of jus in bello, Just War Theory omits an important way senior political and military leaders can fail to meet wartime responsibilities.

Setting conditions for fulfilling those responsibilities requires getting the civilian-military relationship right. Dubik argues that two dominant views, those of Samuel Huntington and Peter Feaver, fail in this regard. Huntington's approach, known as "objective control," divides responsibility much along the same lines as traditional Just War Theory: the civilian leadership is responsible for deciding when to go to war, while the military leadership is responsible for fighting it. The problem with this approach is that the demarcation line between purely political and purely military can be blurry. It is not in the interests of the political leadership to leave all the war-making decisions to the military, as Abraham Lincoln found out when he entrusted the war to George McClellan. Moreover, especially in the United States where the military is accountable both to the President and Congress, it is not always possible for the military to stay out of the political side of war.

Unfortunately, Feaver's "principal agent" approach, while an improvement, does not fare much better. This approach, which recognizes that political and military leaders can have experience relevant to both spheres, characterizes the civilian-military relationship as that of employer

to employee, where the key role of the civilian is to ensure the military does what missions the civilian leadership assigns—and in the manner the civilian leadership wants it done.

The advantage of this approach is that it establishes a dialog between the two spheres that allows for greater alignment among policy, strategy, and execution; however, by placing the ultimate responsibility on the civilian side, it gives the civilian the "right to be wrong," while letting the military somewhat off the hook. Certainly, the military can be held accountable for the decisions it makes, but the internal dynamics of power, control, and obedience can obstruct the dialog it seeks to introduce. Moreover, the compliance monitoring such an approach entails inhibits the kind of adaptation necessary for good war-waging. Finally, and perhaps most importantly, it ignores the obligations civilian leadership has to soldiers, who are themselves citizens and to whom some due care should be owed. This view does not entail that civilian leaders are not accountable, only that they are accountable to the voters, not to the military or for the soldiers' lives they may sacrifice.

While Dubik approves of the deliberative dynamic the principal-agent approach introduces, he argues that a "civil-military relationship based on power and control is not the kind of relationship necessary to wage war." Aligning war aims, strategies, policies, and campaigns in a way that has the highest chance for success requires a more equal dialog and one where no party has a right to be wrong.

The approach that Dubik favors, which he describes as the "decision-execution regime," is one he draws from Eliot Cohen's idea of "unequal dialog." In such a dialog, both civilian and military leaders hold each other accountable for the decisions they make through a process Dubik describes variously as repetitive, overlapping, tense, and conflictual but that provides space for the "incessant, close, difficult questioning of positions, assumptions, and suggested courses of action." The dialog is unequal only that at some point it must end and it is ultimately the civilian authority—if not the circumstances under which some decision is considered—who gets to say when. No right to be wrong.

Governing that dialog are five principles Dubik argues should have the same status in Just War Theory as the principles of discrimination and proportionality have in traditional accounts of jus in bello. Summarized, these principles call for continuous dialog from the outset; extension of the civilian's "final authority" to war-waging; managerial competence on the part of all parties to employ the bureaucracy to achieve the established war aims; maintenance of legitimacy by fighting the war not only justly but also in a manner that provides the highest probability of success; and resignation, when the collective leadership fails to live up to these principles and thus their responsibilities.

Overall, Dubik makes a compelling case regarding senior civilian and military leadership accountability for waging war. His account masterfully addresses what counts as mistakes and what counts as moral failures and suggests a process to minimize both. However, it does seem odd that the principles he articulates should feature as part of the Just War tradition, which involves the mutual upholding of norms associated with both going to war and the actual fighting. As Robert Vicars notes in his review of the book, the best way to determine the relevance of Dubik's view to Just War Theory is to ask the question, "Is this how I want my enemy to act in war?" The answer is, arguably, no.

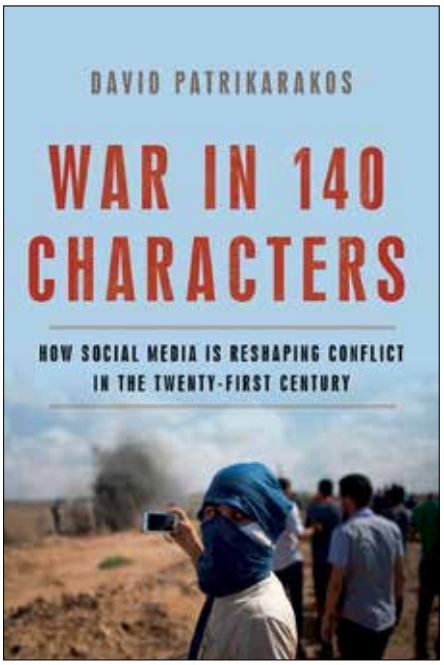
So while Dubik makes a good case for holding leaders accountable to their publics, it is not clear that these principles have the same status within the context of Just War as the traditional principles do.

While Dubik did not fully develop a response to this concern, he laid the groundwork for a response. First, he observes that those waging war engage in multiple relationships. First is with the innocent, to whom they must show due care; second is among soldiers themselves, whose trust in each other is an essential feature of a successful military; third is that of military leaders with their soldiers, for whom they must balance their humanity along with their instrumentality to successfully achieving war aims; and fourth, the "citizens-who-become-soldiers" to their senior political and military leaders, who owe them due care when making decisions associated with waging war.

The question here is whether Just War Theory can make room for the asymmetries of these different relationships. There is precedent in the theory to suggest that it can. One relationship Dubik did not mention was the relationship soldiers have with enemy soldiers. In fairness, this would obviously be a very thin relationship; however, it does entail some obligations, such as avoiding unnecessary harm, use of impermissible weapons, and acceptance of surrender, among others. These are different obligations than what soldiers have to enemy civilians, whom they are supposed to avoid targeting altogether. So at a rudimentary level, Just War Theory accommodates the kind of asymmetries that Dubik proposes, so it should not be too much of a leap to broaden the scope and scale of those asymmetries to accommodate Dubik's principles.

Wherever one falls out on the proper scope of Just War Theory, James Dubik makes a compelling case that an ethic of waging war is as essential to a full accounting of moral responsibilities in war as the ethics of jus ad bellum and jus in bello. As such, it is critical reading for national security professionals who are in positions where they will make or advise those who make decisions regarding waging war. **JFQ**

Dr. C. Anthony Pfaff is a Faculty Member at the U.S. Army War College and has recently completed a detail on the National Security Council.



War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century
By David Patrikarakos
Basic Books, 2017
$30.00 320 pp.
ISBN: 978-0465096145

Reviewed by Brett Swaney

How has social media reshaped war and the way it is fought? That is the question at the heart of David Patrikarakos's *War in 140 Characters*, in which he asserts that social media has reshaped not only the battlefield but also, more importantly, the discourse surrounding it. It is a new paradigm that many are only just beginning to explore.

Central to Patrikarakos's thesis is the shifting balance of power between the individual and state. This is the axis around which the narrative unfolds. Patrikarakos argues principally that the decentralization of information through social media networks has eroded institutional and state control over information flows, and thus the narratives in conflict and the discourse around war. All wars, he argues, are essentially a clash of narratives, echoing a point stressed by General James Mattis during his time in Iraq and by Sir Lawrence Freedman, Emeritus Professor of War Studies at King's College London.

As a journalist navigating modern conflicts in Ukraine and Israel-Palestine, Patrikarakos draws on his personal observations to illustrate the ways in which war has been reshaped by social media. The reader is introduced to *homo digitalis*, the hyper-empowered, social media networked individual. Homo digitalis includes individuals such as Farah Baker, a Palestinian teenager with a global audience; Anna Sandalova, a Facebook warrior with an agile volunteer network in Ukraine; and Vitaly Bespalov, a Russian youth caught up in the Kremlin's information war in Ukraine as a digital troll. These are just some of the portraits Patrikarakos sketches to illuminate individuals, frequently noncombatants, with the power to influence the course of conflict on and off the battlefield.

Patrikarakos suggests that in the information domain, influencers like Baker are able to bypass traditional gatekeepers (old television and print news media and the state) to reach a global audience that can impact the political calculus of an adversary. During the 2014 Israel-Hamas conflict, Farah (and many like her) helped strengthen international outrage against Israel and highlight Palestinian suffering. While it did not influence the movement of tanks or targets of rockets, it appeared to affect the perceived legitimacy of Israel's use of force globally, something the Israeli Defense Forces (IDF) took seriously.

While Patrikarakos argues that social media has diluted the power of the state and empowers the individual, on balance, he is careful to address how some states are working hard to adapt and control the narrative in conflict. Russia is singled out for morbid praise as a state that has boldly embraced the new paradigm, bending the power of social media to construct narratives that convince and reassure supporters while sowing confusion among adversaries. Patrikarakos leaves the reader with a warning: "The world has not yet caught up with Russia; it still believes that words, propaganda, and partisan narratives are less dangerous than tanks."

Patrikarakos concludes that the IDF cannot stop Farah, the National Security Agency cannot stop WikiLeaks, and the Center for Strategic Counterterrorism Communications cannot stop the virtual so-called Islamic State. This is a key insight: the principal actors shaping the discourse around war and the legitimacy of conflict have evolved. They are no longer just states and sprawling media institutions; they must now compete with innumerable, empowered individuals.

For Clausewitzian-minded readers, Patrikarakos argues, provocatively, that as the line between war and politics becomes blurred, the Clausewitzian paradigm becomes less relevant. In a world in which the state does not have a monopoly on information flows, one side can win militarily, but lose politically. The practice of war, he claims, has not changed, but the *context* in which it takes place has.

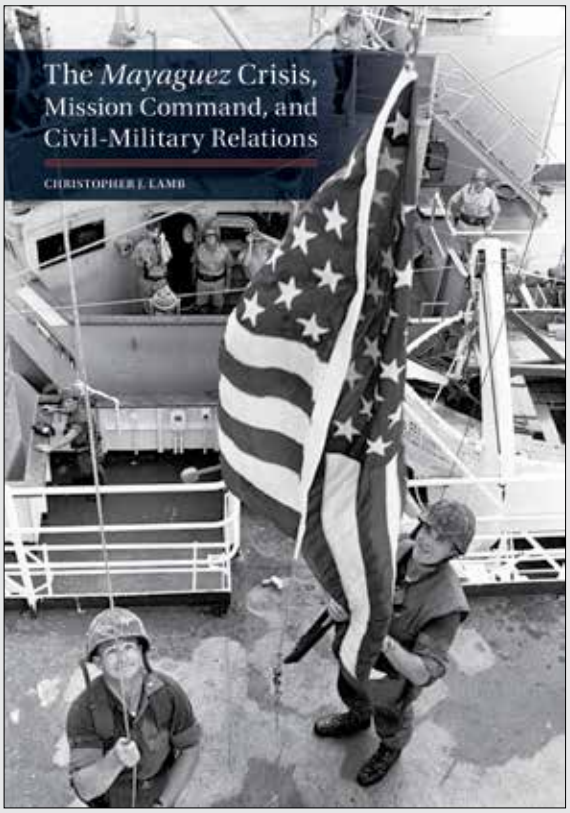
Patrikarakos returns to the Gaza conflict in 2014 as an example of a clear military victory but a political defeat due to the altered context. Israel successfully bombed and invaded Gaza, the tunnel threat was reduced, and the rocket attacks nearly halted. However, the backlash to the conflict by a global audience, especially in Europe and the United States, turned military achievements into a political crisis of legitimacy in conflict.

Strategists and historians will undoubtedly find much to chew on here, and likely take issue with the author's characterization of the Clausewitizan paradigm as a "classic" way of war with clear "political settlements" when the dust settles. Indeed, many will find Clausewitz highly relevant to the evolving context in which war takes place. A careful reading of Clausewitz will reveal that war's political purpose is the "supreme consideration" that must "permeate all military operations" and have "a continuous influence on them." In that sense, the real issue may not be the narrative around conflict, but rather the failure of Israel to accurately understand and adapt its political aims relative to the larger context and impact of military action.

For national security professionals of all stripes, *War in 140 Characters* offers a compelling depiction of contemporary conflict increasingly shaped by homo digitalis. Indeed, Patrikarakos convincingly argues that the state's power over information flows and the discourse around conflict has eroded, resulting in a wave of new actors in war. This book is an important deep dive for any national security professional who seeks a better understanding of the power and peril of social media.

Ultimately, the hypothesis about whether the nature of conflict has fundamentally changed remains unproved, but David Patrikarakos does a wonderful job demonstrating how social media has empowered new actors during war, peace, and the gray zone in between. Arguably, he succeeds in his core task of demonstrating that homo digitalis is a powerful new phenomenon shaping war and politics in the 21st century. **JFQ**

Brett Swaney is a Research Analyst in the Institute for National Strategic Studies at the National Defense University.



New from the Office of Joint History

The Mayaguez Crisis, Mission Command, and Civil-Military Relations

By Christopher J. Lamb
2018 • xxiv + 284 pp.

President Gerald R. Ford's 1975 decision to use force after the Cambodians seized the USS *Mayaguez* merchant ship is one of the best documented but least understood crises in U.S. history. U.S. behavior is still explained as a rescue mission, a defense of freedom of the seas, an exercise in realpolitik, a political gambit to enhance Ford's domestic political fortunes, and a national spasm of violence from frustration over losing Vietnam. Widespread confusion about what happened and why it did contributes to equally confused explanations for U.S. behavior.

Now, with new sources and penetrating analysis, Christopher J. Lamb's *The Mayaguez Crisis, Mission Command, and Civil-Military Relations* demonstrates how three decades of scholarship mischaracterized U.S. motives and why the common allegation of civilian micromanagement during the crisis is wrong. He then extracts lessons for current issues such as mission command philosophy, civil-military relations, and national security reform. In closing he makes the argument that the incredible sacrifices made by U.S. Servicemen during the crisis might have been avoided but were not in vain.

U2 Dragon Lady pilot with 5th Reconnaissance Squadron waits in pressure suit before flight at Osan Air Base, South Korea, December 11, 2018 (U.S. Air Force/Sergio A. Gamboa)

Master and Commander in Joint Air Operations

Winning the Air War Through Mission Command

By Matthew Quintero

But in case signals can neither be seen [n]*or perfectly understood, no Captain can do very wrong if he places his Ship alongside that of an Enemy.*

—Vice Admiral Horatio Nelson

While planning for the battle of Trafalgar, Vice Admiral Nelson had an ingenious idea. He would break from doctrine—risking command and control (C2) of his fleet—and part his line of ships into two columns to drive directly at the enemy and force a decisive engagement. Success required trust in his captains to execute the intent of his plan in the heat of battle when they could no longer see his flagship's signals. Nelson's intent was clear: his forces were to find the enemy and engage them. Clear commander's guidance, nonreliance on communications between the tactical commander and the operational commander, autonomous execution of mission-type orders, and, most impor-

Lieutenant Commander Matthew Quintero, USN, is a Naval Flight Officer and E-2D Mission Commander. He is currently a Resident Student at the U.S. Naval War College.

tantly, the trust between the commander and his subordinates to execute those orders within his guidance are the hallmarks of a concept as old as Nelson—mission command. Mission command is described in joint doctrine as follows:

If a commander loses reliable communications, mission command—a key component of the C2 [joint] *function—enables military operations through decentralized execution based on mission-type orders. Commanders delegate decisions to subordinates wherever possible, which minimizes detailed control and empowers subordinates' initiative to make decisions based on the commander's guidance rather than constant communications.*[1]

While mission command is not a new concept, much has been written on the topic since 2012 when then–Chairman of the Joint Chiefs of Staff General Martin Dempsey released his white paper, *Mission Command*, which implored his subordinates to "live and breathe" that style of command and control.[2] In 2014, Joint Publication (JP) 3-30, *Command and Control of Air Operations*, was updated to include a discussion of mission command.[3]

Since the advent of satellite communications and the Internet, C2 of joint air operations has become increasingly centralized. Today's far-reaching C2 systems allow operational commanders to make tactical-level decisions from thousands of miles away. Although JP 3-30 discusses the virtues of mission command, it goes on to explain that joint air operations have unique qualities that are not always fit for mission command. JP 3-30 explicitly provides for times when a high degree of centralized control and tactical oversight is desired for an operation. Moreover, it details requirements for "robust command and control systems" to enable that oversight. While these C2 systems may be untenable in future operating environments against a capable foe, the uncontested air environments of Operations *Southern Watch* (OSW), *Desert Storm* (ODS), *Enduring Freedom* (OEF), and *Iraqi Freedom* (OIF) have allowed this way of C2 to thrive. Proponents of this trend argue that lack of centralized control may "result in failure to capitalize on joint force integration or may degrade operational-level flexibility," especially in the cases of "sensitive strikes."[4]

It seems doctrine has forgotten the hard-learned lessons of past air campaigns, specifically the war in the Pacific, where mission command was instrumental in America's victories over formidable Japanese air forces. Likewise, there are no discussions of the most important enablers of mission command, such as trust, delegation, initiative, and commander's intent.[5] These are intangible leadership qualities required of a joint force air component commander (JFACC).

To win America's future air wars, mission command must be woven into the fabric of joint air operations. To prove this assertion, this article first establishes the validity of mission command in major air operations by considering the the Battle of Midway. Then, the efficacy of modern communications technology, which allows centralized C2, is challenged by looking forward to America's potential adversaries. Finally, the article's focus is turned to today's operational leadership challenges and the importance of the JFACC as the key enabler of successful mission command.

Midway: America's Trafalgar

The Battle of Midway is regarded as a prime example of an American air battle where the operational commander successfully employed the principles of mission command. Like Nelson at Trafalgar, Admiral Chester Nimitz, the operational commander, had a clear concept of operations that capitalized on the trust of his subordinates and required little in the way of C2 communications.[6] Nimitz trusted his intelligence officers who predicted a Japanese invasion force at Midway Island, and his intent for the defense of the island was clearly communicated via his Operation Plan (OPLAN) 29-42.[7] The plan was well-communicated through the distribution of 86 hardcopies to his carrier battle groups and the Army air forces on Midway.[8]

During the battle and the days leading up to it, Nimitz made few C2 communications due to necessity, the strength of his plan, and the trust he placed in Admirals Raymond Spruance and Frank Fletcher, his subordinate carrier commanders.[9] To prevent detection by Japanese radio direction-finding technology before the battle, Spruance and Fletcher were restrained to visual signals, and Nimitz could only broadcast messages to his fleet. Once the battle began, Nimitz knew to expect incomplete information at best.[10] Nimitz retained operational control over his naval forces and the Army air forces on Midway Island. Tactical control of the battle was left to Fletcher.[11] Once the OPLAN was put in place, he refrained from further involvement in the battle. Success required that Nimitz trust his subordinate commanders to execute his vision. Japanese technology and, more importantly, the imminent threat of Japanese invasion did not allow Nimitz any other options but to completely release tactical control to his subordinates. Regardless, American victory at Midway is largely attributed to Nimitz's leadership. U.S. air forces have not fought an evenly matched opponent since World War II, and there has been no impetus for C2 through mission command in subsequent conflicts. Generations of commanders have since faced lower intensity operations, allowing levels of centralized C2 to be unsustainable in a conventional war.

Current joint air operations do not exhibit the right attitude for waging an air campaign against a capable foe. America's last three major air campaigns—ODS, OEF, and OIF—have all been marked both in doctrine and execution by an increased reliance on C2 systems to make decisions. JP 3-30 has evolved from the tenant of "centralized planning, and decentralized execution" to "centralized control and decentralized execution."[12] JP 3-30 further explains that "specific missions and capabilities will drive . . . the extent that mission-type orders may be used." JP 3-30 also explains that "Highly sensitive strike missions . . . will generally require a higher level of detailed planning and centralized

F/A-18F Super Hornet assigned to Air Test and Evaluation Squadron (VX) 23 flies over aircraft carrier USS *Gerald R. Ford*, July 28, 2017, in Atlantic Ocean (U.S. Navy/Erik Hildebrandt)

control."[13] The pitfall associated with this trend is the reliance on C2 systems rather than commander's intent. A joint force commander or component commander must anticipate the actions of the enemy and affect the future of an operation. This cannot be accomplished by merely reacting to C2 systems.[14] In a future fight for air supremacy against a determined enemy, access to advanced C2 systems will not be assured, and the sheer number of timely decisions required will make any type of centralized C2 unsustainable.

C2 Systems: The Enablers of Centralization

The JFACC will not be able to conduct business as usual in a fight with an enemy that has the capability to disrupt C2, whether it is due to low-cost harassment of computer and satellite systems or fear of high-end missile attacks. With its enormous network and satellite communications capabilities, the Joint Air and Space Operations Center (JAOC) is the heart of the joint air C2 system. With the ability to reach back to critical information sources stateside and reach forward to individual aircraft in theater, the JAOC is a powerful tool for the JFACC. This C2 system has worked well for planning major air campaigns in ODS, OEF, and OIF, but it has met shortfalls when trying to communicate with air controllers on the ground, ships at sea, and aircraft over the battlefield. The JAOC is unproved against an enemy actively working to degrade the Internet and satellite capabilities that enable it. Furthermore, it will be unable to closely control tactical units, especially carrier-based aircraft, when those units voluntarily block off communications to remain undetected.

In the future, persistent access to safeguarded networks cannot be assumed. At the onset of OEF, the JAOC in Saudi Arabia was a technological marvel of C2 capability, described as "how war rooms are depicted in Hollywood movies."[15] Vast amounts of information collected from both sensors on the battlefield and sources back in the United States were available to the JFACC. These huge amounts of data traveled over secure Internet lines.[16] Since the start of OEF, these internet networks have proved vulnerable to computer network attacks (CNA).[17] In the case of SIPRNet (secret-level Internet), it has since been breached by a virus transmitted from a USB thumb drive at a terminal in Afghanistan. Of note, email accounts within the Pentagon, including those belonging to the Joint Chiefs of Staff, were compromised due to this attack from the far side of the world.[18]

Like Nimitz with his 86 hardcopies of his OPLAN, joint air C2 can overcome CNA through mission command principles. Reliance on high-capacity networks for C2 is seen as a critical vulnerability

that our adversaries are actively planning on. According to one report, "Chinese writings reveal an interest in the full spectrum of CNA tools, including hacking, viruses, physical attack, insider sabotage, and electromagnetic attack."[19] That report also states, "Chinese CNA targeting focuses specifically on enemy C2 centers." The same report brings up some interesting points that could be exploited through mission command. First, some Chinese writings argue that U.S. command and control will be unable to operate without their computer systems. It further states that "Chinese strategists generally underestimate the capacity of the system to use paper, pencil, fax, and phone if necessary."[20] Also of interest is an assessment that "Chinese writings on information warfare show no confidence in China's ability to get inside . . . deployed ships or other self-contained operational units."[21] Through independent action without instant information, and reliance on older methods of communications, the United States can maintain the advantage in the face of sophisticated network attacks.

Any requirements for instant updates from aircraft over the battlefield to the JFACC will be heavily reliant on satellite communications (SATCOM), which have historically proven inadequate during major combat operations. During ODS, to connect U.S. Central Command (USCENTCOM) in Tampa, Florida, to the battlefield, SATCOM was required between not only Tampa and the JAOC in theatre but also the JAOC and key "air control" platforms such as the E-2 Hawkeye, E-3 Sentry, and E-8 JSTARS.[22] These aircraft then maintained line-of-sight communications with hundreds of aircraft in theatre. At the onset of ODS, this envisioned SATCOM capacity did not exist, and the existing capacity was quickly overloaded.[23] Additionally, with SATCOM as their primary source of computer file exchange and long-range communications, the United States and allied forces at sea were often left in the dark. S-3 Vikings from the carriers were required to transport hardcopies of vital JFACC orders for flight planning such as the Air Tasking Order (ATO).[24] Commercial satellite systems were brought in to fill the gaps. In fact, at the "height of *Desert Storm* over 95 percent of [US]CENTCOM's long-range communications were handled by satellite communications with only 72 percent on military satellites."[25] Eleven years later during OIF, SATCOM capabilities proved inadequate in connecting end users to the JFACC. When tactical air control parties on the ground could not maintain communications with the JAOC, E-2s and E-3s stepped in to provide live coordination of tasking, aerial refueling, battle damage assessment, and restrikes between the Combined Air Operations Center (CAOC) and tactical aircraft flying in theatre.[26] Twenty-seven years later, E-2s and E-3s still use the same commercial SATCOM systems for long-range communications. Moreover, these SATCOM paths are now being used to bring Internet capabilities to the aircraft.[27] Long-range communication shortfalls and congestion occurred when SATCOM use was completely uncontested. Adversaries rightfully see this as a critical vulnerability of C2 and it is subject to exploitation. A *Chinese Liberation Army Daily* article states, "Anti-satellite weapons that can be developed at low cost and that can strike at the enemy's enormously expensive yet vulnerable space system will become an important option for the majority of medium-sized and small countries with fragile space technology."[28] Furthermore, Chinese strategic writings have argued the following:

> *The enemy's naval force and its national military command authorities, naval command centers, and other force links mainly rely on high frequency satellite communications . . . including commercial and military satellite communications, all of which are easily susceptible to electronic interference and deception.*[29]

SATCOM will not be guaranteed in an uncontested environment, much less a contested one. C2 through mission command can relieve the impact of degraded SATCOM. Through well-written mission-type orders, we can place decisionmaking in the heads and hands of our aircraft over the battlefield.

Compounding the communications problem, future naval air forces will operate from self-imposed emissions restrictions. As long-range enemy missile technologies advance, naval forces will operate for days, weeks, or months in highly restrictive electromagnetic spectrum emissions control (EMCON) statuses in order to prevent the enemy from locating and targeting its ships.[30] Like Spruance and Fletcher at Midway, today's commanders will need to fight and maneuver in silence. For decades, EMCON operations have been the exception and not the rule for the Navy. Ironically, this can be attributed to increasing demand for communications and data paths, which use a large portion of the electromagnetic spectrum.[31] Like Nimitz, the JFACC must give his naval air forces clear intent and guidance before they go EMCON. Then, he must sit back and trust his subordinate commanders to execute that intent.

Mission command can overcome the shortfalls of current C2 systems. Requirements for "robust C2 systems" and their enabling the JFACC to maintain centralized command and control through these systems must be given greater context in JP 3-30. While they are powerful tools in preparing for a conflict, unfettered use of the Internet and SATCOM cannot be expected during a conflict with a skilled adversary. As in the case of the S-3s flying hardcopies of the ATO to the carriers, the JAOC must be ready to use more primitive methods to deliver orders when C2 systems are taken away. Mission command will be essential in the writing of these orders, as the ability to quickly change these orders may be impossible. When communications degraded during OEF and OIF, airborne C2 platforms such as the E-2 and E-3 stepped in to bridge the gap among the JFACC at the JAOC, troops on the ground, and aircraft flying over the battlefield. The usage of airborne C2 platforms should not be limited to air control or radio relay. The JFACC can reduce requirements for long-range communications by allowing increased

levels of decisionmaking to occur within those aircraft. Well-communicated intent channeled through mission-type orders distributed before major combat operations will give America the advantage in future air wars.

JFACC: The Enabler of Mission Command

Success in mission command requires a commander willing to employ it. As General Dempsey stated in his white paper, "mission command is commander-centric."[32] A great deal relies on the personality of the commander. He must have the resolve to confront his own cognitive limitations and the will to place uncomfortable levels of trust in his subordinates. While decisions with potential for strategic consequences may not be in his hands, the JFACC must resolve to do everything in his power to delegate decisionmaking to the lowest levels possible:

Before long distance communications, a commander's span of control was limited to the subordinates who could directly hear his voice. Modern communications allow control over much greater distances. Nonetheless . . . a single commander can only exercise close control over a finite number of other soldiers during a fast-moving battle. And while radios, digitized messages, electronic maps, and symbology have improved upon the human voice in many ways, none of these enhancements has done much to expand the cognitive capacity of the individual tactical commander.[33]

At the onset of OEF, JFACC General Charles Wald compared the amount of information made available to him during a few days at the JAOC as being equivalent to the amount of data collection and research made available to him during 6 months of ODS.[34] With such an abundance of data, the issue now becomes the ability of the commander to filter signal from noise. If the JFACC and his staff focus on fine details at the tactical level, they will not produce content that is necessary for the operational level of warfare. An overabundance of information can ultimately lead commanders to lose sight of what is important to their level of command.[35] Perhaps the most insidious side effect of this overabundance may be the inevitable search for perfect information. The quest to have perfect information in order to make a perfect decision threatens to slow the decisionmaking process to the point of inaction. Trust is threatened when subordinates feel this quest is mere meddling by their commanders.

Persistent sensor coverage and long-range communications systems have enabled tactical micromanagement by operational commanders.[36] Prior to OEF, the JAOC led OSW. OSW policed the Iraqi no-fly zone. USCENTCOM maintained highly centralized control over tactical execution due to the slow pace of the operation. OSW was characterized by a "draconian" set of rules of engagement (ROEs), and the JAOC had to ask USCENTCOM for permission to take any type of enforcement action.[37] In the execution of OEF, USCENTCOM maintained a high level of centralized control reminiscent of OSW through strict ROEs, special instructions (SPINs), and target vetting.[38] ROE during OEF basically required that any target with the potential of collateral damage required approval from USCENTCOM or higher. Reportedly, there were at least 10 times when top Taliban and al Qaeda leadership had been located and placed in the crosshairs of an aircraft during the first 6 weeks of OEF. By the time engagement decisions came back down from USCENTCOM, the opportunity to fire had been lost.[39] More simply stated by a CAOC staffer at the time, "we knew we had some of the big boys. The process [was] so slow that by the time we got the clearances and everybody put in their two cents, we called it off."[40]

OIF ushered in the era of *network-centric warfare* defined as a "systematic approach aimed at improving combat decisionmaking at all levels by creating a seamless grid of interconnected sensors, weapons, individuals, and command and control mechanisms . . . to enhance the ability to sense, locate, communicate, attack, and assess."[41] Or in the case of the air war, it was described as "Internet-in-the-cockpit capability."[42] Once again, the operational commander would have another avenue to reach out and touch the battlefield. Today's JFACC has the time and tools to intervene at the tactical level; the JFACC of the future will not have those tools or time.

The strict ROEs and micromanagement in the OEF example can be defended by the high value placed on preventing civilian casualties and maintaining strategic messaging.[43] ROEs come down from the strategic level of war, and commanders at the operational level must work within the guidance they are given. While centralized control during OEF may have had the best intentions, the unintended consequence was that the "time-sensitive" targets were lost to it. The JFACC must allow the decision to pull a trigger to occur at the lowest tactical levels possible. To do so, he must also advocate for ROEs from higher up that allows decentralization and freedom of action. As the commander of Naval Air Forces concluded at the time, "I think we need to put [the decision authority] back in the cockpit if we are going to enable time-critical strike."[44] The trend of centralizing decisionmaking may work in the uncontested environment of today, but it risks creating a culture that will be hard to change when the United States finds itself fighting an enemy that is capable of contesting it in the sky.

On June 18, 2017, a Navy F/A-18 shot down a Syrian Su-22 in defense of friendly forces on the ground in support of Operation *Inherent Resolve* (OIR). This event marked the only air-to-air shoot-down of enemy aircraft by U.S. forces since Operation *Allied Force* in 1999.[45] When interviewed a few days later, Lieutenant General Jeffrey Harrigian, the Combined Force Air Component Commander (CFACC) and de facto JFACC for OIR, defended the actions of the Navy aircrew. He specifically commented on the need for placing decisionmaking in the cockpit, stating, "when you're doing 400 knots and the adversary is coming at you at 400 knots there is no time for someone from the [JAOC] to tell you what to do. . . . They were going to be the ones that needed to make that self-defense decision."[46]

Airman with 1st Special Operations Logistic Readiness Squadron conducts forward area refueling point operation at Hurlburt Field, Florida, February 26, 2017 (U.S. Air Force/Joseph Pick)

Furthermore, this guidance was clear to the aircrew well before the event. Months later at a panel interview, one of the Navy aircrew involved in the shoot-down stated:

CFACC came out to the aircraft carrier not too many days prior to [the shoot-down] . . . *talking directly to the aircrew . . . saying that "you know my guidance . . . I have your back" . . . emphasizing the point that you have to go out there and operate autonomously within the commander's guidance . . . and your decisions have strategic implications so don't take those decisions lightly.*[47]

And as to the judgment of the pilot who actually pulled the trigger, the aircrew had this to say:

But it cannot be emphasized enough, that . . . to recognize that it was his job . . . to execute the ROE . . . and squeeze the trigger . . . could not have been made possible without our entire command environment from the [commanding officer] *up through* [the commander's action group], *Admiral, and all the way up to the CFACC.*[48]

This event is a shining example of how mission command worked and why it was required. The JFACC made it clear that he trusted the officers who would be flying his missions. Sadly, the actions by the Navy aircrew on that day could arguably be the culmination of one commander's efforts rather than the product of a system set up to achieve mission command. Trusting subordinates is arguably the hardest part of mission command.

In the case of Midway, there was a true existential threat to U.S. forces in the Pacific. By being outnumbered, there was no incentive for Nimitz to intervene at the tactical level. His subordinate commanders would have their hands full in fighting the Japanese carrier fleet. Much like Nimitz, operational commanders cannot expect to approve every engagement in a conflict when hundreds of engagements may be taking place simultaneously. In this effort, the JFACC has powerful tools at his disposal in the form of products such as the ATO and SPINs. Specifically, the SPINs convey the JFACC's intent and meld that with ROEs to give the aircrew a set of instructions to follow in the execution of their missions.[49] The SPINs also provide for times, usually involving air-to-ground or air-to-air engagements, when JFACC approvals must be sought out. Future JFACCs must strive to reduce these occasions or find ways to delegate those approval powers to lower levels. As in OIR, the operational commander must realize the limitations of their own abilities. The JFACC must provide the correct levels of guidance, ROEs, and mission-type orders to allow their subordinates to execute their intent.

Marine controls forward arming and refueling point operations after refueling Bell AH-1W Super Cobra at Pohakuloa Training Area, Hawaii, July 18, 2018 (U.S. Marine Corps/Adam Montera)

Conclusion

To win America's future air wars, mission command must be woven into the fabric of joint air operations. Doctrine must change to accommodate it. Commanders must be willing to employ it. The recent example of mission command in the Su-22 shootdown seems to buck the recent trend of increasing centralization; however, it can arguably be attributed to one determined commander rather than the culture and doctrine that preceded it. JP 3-30 has supported centralization of C2 by calling for C2 systems that allow the JFACC to direct tactical actions over the battlefield and providing times when that may be appropriate. While the JAOC's C2 systems provide powerful tools for information-gathering, overuse risks undermining the value of well-communicated commander's intent and mission-type orders. A skilled adversary will not allow unfettered use of C2 systems that have become customary. Furthermore, doctrine fails to describe the importance of the JFACC in mission command. As in the OIR example, the JFACC must realize the limitations of his own abilities and trust he has provided the correct levels of guidance to allow subordinates to execute intent.

In the future, decisions to engage the enemy will need to be made at the lowest levels. The JFACC may be led to indecision as he attempts to sift through tremendous amounts of information in order to find a perfect answer. If he attempts to maintain centralized C2, he will soon be overwhelmed by the number of decisions to be made. Even if he can make those decisions, the enemy may cut off his means of communicating them. The JFACC must trust his officers, alone in their aircraft, to make the right decisions. Trust is the hardest part of mission command. For the commander struggling with trust when strategic consequences may be at stake, it may help to once again read the words of Vice Admiral Nelson. Far from headquarters and without orders, he had to decide whether or not to engage a shore garrison. He had this to say about his decision:

I have no doubt in the way we proposed to attempt it, by bombardment and cannonading, joined to a close blockade of the harbor. . . . If not . . . our Country will, I believe, sooner forgive an officer for attacking his enemy than for letting it alone.[50] **JFQ**

Notes

[1] Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, 2017), available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0_20170117.pdf>.

[2] Martin E. Dempsey, *Mission Command* (Washington, DC: The Joint Staff, 2012), available at <www.jcs.mil/Portals/36/Documents/Publications/missioncommandwhitepaper2012.pdf>.

[3] JP 3-30, *Command and Control of Joint Air Operations* (Washington, DC: The Joint Staff, 2014), available at <www.dtic.mil/doctrine/new_pubs/jp3_30.pdf>.

[4] Ibid.

[5] Ibid.

[6] Carl H. Builder, Steven C. Bankes, and Richard Nordin, *Command Concepts: A Theory Derived from the Practice of Command and Control* (Santa Monica, CA: RAND, 1999), 38.

[7] Ibid., 39.

[8] Ibid., 42.

[9] Ibid.

[10] Ibid., 38.

[11] James A. Winnefeld and Dana J. Johnson, *Command and Control of Joint Air Operations: Some Lessons Learned from Four Case Studies of an Enduring Issue* (Santa Monica, CA: RAND, 1991), 57.

[12] JP 3-56.1, *Command and Control of Joint Air Operations* (Washington, DC: The Joint Staff, 1994), v; JP 3-30.

[13] JP 3-30.

[14] Builder, Bankes, and Nordin, *Command Concepts*, 2–3.

[15] Benjamin S. Lambeth, *Air Power Against Terror: America's Conduct of Operation Enduring Freedom* (Santa Monica, CA: RAND, 2005), 280.

[16] Ibid.

[17] James A Green, *Cyber Warfare: A Multidisciplinary Analysis* (London: Routledge, Taylor & Francis Group, 2016), 23.

[18] Ibid., 22–23.

[19] James C. Mulvenon, *Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense* (Santa Monica, CA: RAND, 2006), 91.

[20] Ibid.

[21] Ibid., 88.

[22] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, *A League of Airmen: U.S. Air Power in the Gulf War* (Santa Monica, CA: RAND, 1994), 205.

[23] Ibid., 208.

[24] Ibid.

[25] Ibid., 205.

[26] Benjamin S Lambeth, *American Carrier Air Power at the Dawn of a New Century* (Santa Monica, CA: RAND, 2005), 54–55.

[27] *Selected Acquisition Report: Airborne Warning and Control System Block 40/45 Upgrade (AWACS Blk 40/45 Upgrade)*, Executive Services Directorate, available at <www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/16-F-0402_DOC_13_AWACS_Blk_40-45_Upgrade_DEC_2015_SAR.pdf>; *Selected Acquisition Report: E-2D Advanced Hawkeye Aircraft (E-2D AHE)*, Executive Services Directorate, available at <www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/16-F-0402_DOC_68_E-2D_AHE_DEC_2015_SAR.pdf>.

[28] Mulvenon, *Chinese Responses*, 68.

[29] Ibid., 71.

[30] Zachary Hoyt, "Get Used to EMCON," U.S. Naval Institute *Proceedings* 143, no. 7 (July 2017), available at <www.usni.org/magazines/proceedings/2017-07/professional-notes%E2%80%94get-used-emcon>.

[31] Ibid.

[32] Dempsey, *Mission Command*.

[33] John Patrick White and Zalmay Khalilzad, *Strategic Appraisal the Changing Role of Information in Warfare* (Santa Monica, CA: RAND, 1999), 161.

[34] Lambeth, *Air Power*, 280.

[35] James Kahan, *Understanding Commanders' Information Needs* (Santa Monica, CA: RAND, 2000), 32.

[36] Lambeth, *Air Power*, 296.

[37] Ibid.

[38] Ibid., 297–298.

[39] Ibid., 314.

[40] Ibid., 314–315.

[41] Lambeth, *American Carrier*, 96.

[42] Ibid., 97.

[43] Lambeth, *Air Power*, 320.

[44] Ibid., 349.

[45] Jim Michaels, "Attacks Heighten Complexity of Air War in Syria," *USA Today*, June 23, 2017, available at <www.usatoday.com/story/news/world/2017/06/23/attacks-air-war-assad-syria/424609001/>.

[46] Ibid.

[47] Jeff Krueger, "Panel # 2—JO Panel—from Tailhook 2017 Symposium," *Livestream.com*, n.d., available at <https://livestream.com/wab/tailhook2017/videos/162478715>.

[48] Ibid.

[49] JP 3-30.

[50] Alfred Thayer Mahan, *The Life of Nelson: The Embodiment of the Sea Power of Great Britain* (Boston: Little, Brown and Co., 1897), 128.

Marines and members of Georgian military participate in combined forces counterinsurgency and peacekeeping operations training exercise Agile Spirit 16 at Orpholo Training Area, Georgia, September 3, 2016 (U.S. Marine Corps/Kyle C. Talbot)

Joint Publication 3-24, *Counterinsurgency*

Joint Publication (JP) 3-24, *Counterinsurgency*, provides joint doctrine to plan, execute, and assess counterinsurgency operations. JP 3-24 defines *counterinsurgency* (COIN) as "comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes." Accordingly, JP 3-24 provides the joint force with authoritative doctrine relative to counterinsurgency by discussing approaches to it, describing the nature of an insurgency, discussing COIN tenets, providing considerations for COIN planning, describing the COIN operational environment, and discussing aspects for the conduct of an assessment.

The Joint Staff director, Joint Force Development J7, signed a revised JP 3-24 on April 25, 2018. JP 3-24 is a priority joint publication supporting joint force requirements relative to COIN operations and in support of threats identified in the National Defense Strategy and National Military Strategy.

The revision was informed by a formal assessment conducted in September 2016 by the Joint Staff J7 Joint Doctrine Analysis Division in Suffolk, Virginia. The assessment represents an analysis of comments received from the Services, combatant commands, Joint Staff directorates, and combat support agencies; search results from joint operations and exercises; lessons learned; and other databases. Many of the changes made to JP 3-24 ensure the publication contains the most current figures, terms, definitions, and references based on changes to other JPs in the joint doctrine library since approval of the 2013 version of JP 3-24. Overall, changes to this revision of JP 3-24:

- reduce redundancy with JP 5-0, *Joint Planning*, by deleting paragraphs addressing the operational assessment model and operational assessment steps

- replace the phrase *generational engagement* with *generational approach* to better reflect long-term partnering as well as engagement
- replace the phrase *counterinsurgency environment* with *operational environment*
- revise the phrase *violent extremist* to include *violent extremist organizations*
- revise the phrase *root causes of the insurgency* to *roots of the insurgency*
- update paragraphs to delineate between information operations and military information support operations
- add a discussion on the roles of women in an insurgency, such as combatants, members of the auxiliary, and suicide bombers
- add a more in-depth discussion on disarmament, demobilization, and reintegration, and how these can be applied while an insurgency is ongoing and after it ends
- add a discussion on criminal networks within COIN operations.

Changes to JP 3-24 are found in each chapter, but the preponderance and most significant changes are found in chapter VII, "Counterinsurgency Operations," and appendix C, "Counterinsurgency Practices." Chapter VII has been rewritten, broken into two sections, and includes 12 new paragraphs, many of them information-related that provide additional context for counterinsurgency operations. Significant changes include:

- Paragraph 1, a general overview emphasizing the need for a synchronized application of military, paramilitary, diplomatic, political, economic, law enforcement, psychological, and civic actions.
- Paragraph 2, "Support the Counterinsurgency Narrative," discusses how operations appropriately aligned with a narrative are strengthened through sense of purpose, unity of effort, and the ability to gain and maintain initiative against insurgents.
- Paragraph 4, "Command and Control," discusses how the command and control function encompasses a number of tasks, as articulated in JP 3-0, *Joint Operations.*
- Paragraph 6, "Operational Methods for Counterinsurgency," discusses several options to consider when conducting COIN operations (generational approach, network engagement, and so forth).
- Paragraph 13, "Targeting," shows how the targeting process can support information-related activities, civil-military operations, and meetings between commanders and host-nation leaders.
- Paragraph 14, "Localized Security Activities," explains that strategic localized security areas may deny the insurgency access to necessary sustainment resources such as food commodities, communications networks, and funding.
- Paragraph 15, "Fires and Joint Fire Support," discusses when conducting COIN operations, a commander may place additional constraints on fires beyond what might be legally required to avoid collateral damage that might bolster support for the insurgency.
- Paragraph 16, "Commander's Communication Synchronization," is a process to coordinate and synchronize themes, messages, operations, and actions with all instruments of national power, and is a way to ensure the integrity and consistency of themes and messages.
- Paragraph 20, "Counterterrorism Operations," discusses ways and means of counterterrorism operations to combat elements of an insurgency that use terrorism as a means to influence local, domestic, and international audiences.
- Paragraph 21, "Electronic Warfare," discusses how electronic warfare may be necessary during COIN operations to protect friendly operations in the electromagnetic spectrum against insurgents who may operate with unsophisticated electronic means.
- Paragraph 27, "Countering Threat Networks," notes the worldwide emergence of adaptive threat networks and the associated challenges to the joint force. Threat networks may be adversarial to COIN forces or may simply be criminally motivated, increasing instability in a given operational area.
- Paragraph 33, "Violent Extremism," discusses how violent extremism and insurgency share many of the same core grievances, but they differ in their degree of organizational support base and the use of violence.
- Appendix C, "Counterinsurgency Practices," is based on a RAND study and provides a list of successful and unsuccessful COIN practices that the joint force commander should take into account when planning for counterinsurgency.

JP 3-24 provides current, authoritative doctrine for the joint force conducting COIN operations. It is a more information-enabled JP 3-24, providing joint force commanders and their component commanders with joint doctrine to plan, execute, and assess COIN operations.

The revised version of JP 3-24 is available at <www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/>. **JFQ**

From NDU Press

Women on the Frontlines of Peace and Security

Foreword by Hillary Rodham Clinton and Leon Panetta

NDU Press, 2015 • 218 pp.

This book reflects President Barack Obama's commitment to advancing women's participation in preventing conflict and keeping peace. It is inspired by the countless women and girls on the frontlines who make a difference every day in their communities and societies by creating opportunities and building peace.

When women are involved in peace negotiations, they raise important issues that might be otherwise overlooked. When women are educated and enabled to participate in every aspect of their societies—from growing the economy to strengthening the security sector—communities are more stable and less prone to conflict.

The goal of this book is to bring together these diverse voices. As leaders in every region of the world recognize, no country can reach its full potential without the participation of all its citizens.

Available at ndupress.ndu.edu/Books/WomenontheFrontlinesofPeaceandSecurity.aspx

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 2-0, *Joint Intelligence*

JP 3-05, *Special Operations*

JP 3-05.1 *Unconventional Warfare*

JP 3-07.4, *Counterdrug Operations*

JP 3-16, *Multinational Operations*

JP 3-17, *Air Mobility Operations*

JP 3-30, *Command and Control for Joint Air Operations*

JP 3-40, *Counter Weapons of Mass Destruction*

JP 3-52, *Joint Airspace Control*

JP 3-72, *Nuclear Operations*

JP 4-10, *Operational Contract Support*

JP 6-0, *Joint Communications System*

JPs Revised (signed within last 6 months)

JP 1, *Doctrine for the Armed Forces of the United States*

JP 3-02, *Amphibious Operations*

JP 3-06, *Joint Urban Operations*

JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*

JP 3-15.1, *Counter–Improvised Explosive Device Operations*

JP 3-28, *Defense Support to Civil Authorities*

JP 3-29, *Foreign Humanitarian Assistance*

JP 3-57, *Civil-Military Operations*

JP 3-60, *Joint Targeting*

JP 4-0, *Joint Logistics*

JP 4-01.5, *Joint Terminal Operations*

JP 4-04, *Contingency Basing*

JP 4-05, *Joint Mobilization Planning*

JP 4-09, *Distribution Operations*

CALL FOR ENTRIES

for the

2019 Secretary of Defense and
2019 Chairman of the Joint Chiefs of Staff

Essay Competitions

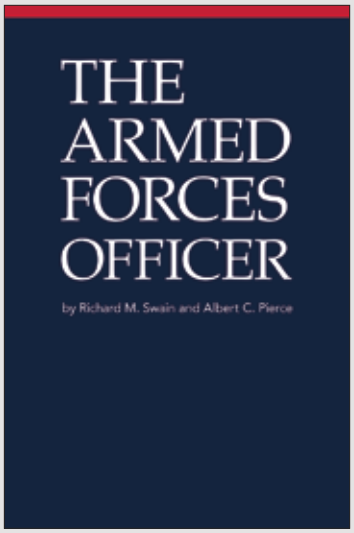
Are you a professional military education (PME) student? Imagine your winning essay published in a future issue of *Joint Force Quarterly*, catching the eye of the Secretary and Chairman as well as contributing to the debate on an important national security issue. These rewards, along with a monetary prize, await the winners.

Who's Eligible? Students, including international students, at U.S. PME colleges, schools, and other programs, and Service research fellows.

What's Required? Research and write an original, unclassified essay on some aspect of U.S. national, defense, or military strategy. The essay may be written in conjunction with a course writing requirement. Important: Please note that entries must be selected by and submitted through your college.

When? Anytime during the 2018–2019 academic year. Students are encouraged to begin early and avoid the spring rush. Final judging and selection of winners take place May 2019, at NDU Press, Fort McNair, Washington, DC.

For further information, see your college's essay coordinator or go to:
http://ndupress.ndu.edu/About/Essay-Competitions/



New from NDU Press

The Armed Forces Officer

2017 • 212 pp.

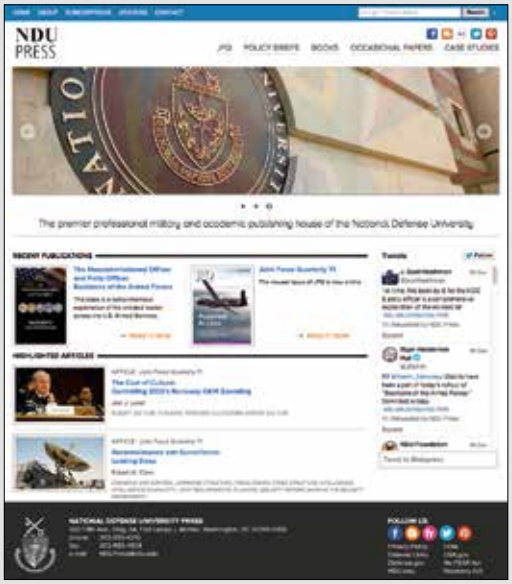
From the Foreword by General Joseph F. Dunford, Jr., Chairman of the Joint Chiefs of Staff:

"In 1950, the great Soldier-Statesman George C. Marshall, then serving as the Secretary of Defense, signed a cover page for a new book titled *The Armed Forces Officer*. That original version of this book was written by none other than S.L.A. Marshall, who later explained that Secretary Marshall had 'inspired the undertaking due to his personal conviction that American military officers, of whatever service, should share common ground ethically and morally.' Written at the dawn of the nuclear age and the emergence of the Cold War, it addressed an officer corps tasked with developing a strategy of nuclear deterrence, facing unprecedented deployments, and adapting to the creation of the Department of Defense and other new organizations necessary to manage the threats of a new global order.

"This new edition of *The Armed Forces Officer* articulates the ethical and moral underpinnings at the core of our profession. The special trust and confidence placed in us by the Nation we protect is built upon this foundation. I commend members of our officer corps to embrace the principles of this important book and practice them daily in the performance of your duties. More importantly, I expect you to imbue these values in the next generation of leaders."

Available at ndupress.ndu.edu/Media/News/Article/1159223/the-armed-forces-officer/

Have you checked out NDU Press online lately?



With 20,000 unique visitors each month, the NDU Press Web site is a great place to find information on new and upcoming articles, occasional papers, books, and other publications.

You can also find us on:

Facebook **Flickr**

Twitter **Pinterest**

Visit us online at: **http://ndupress.ndu.edu**

JFQ is available online at the Joint Electronic Library:
www.dtic.mil/doctrine/jfq/jfq.htm

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