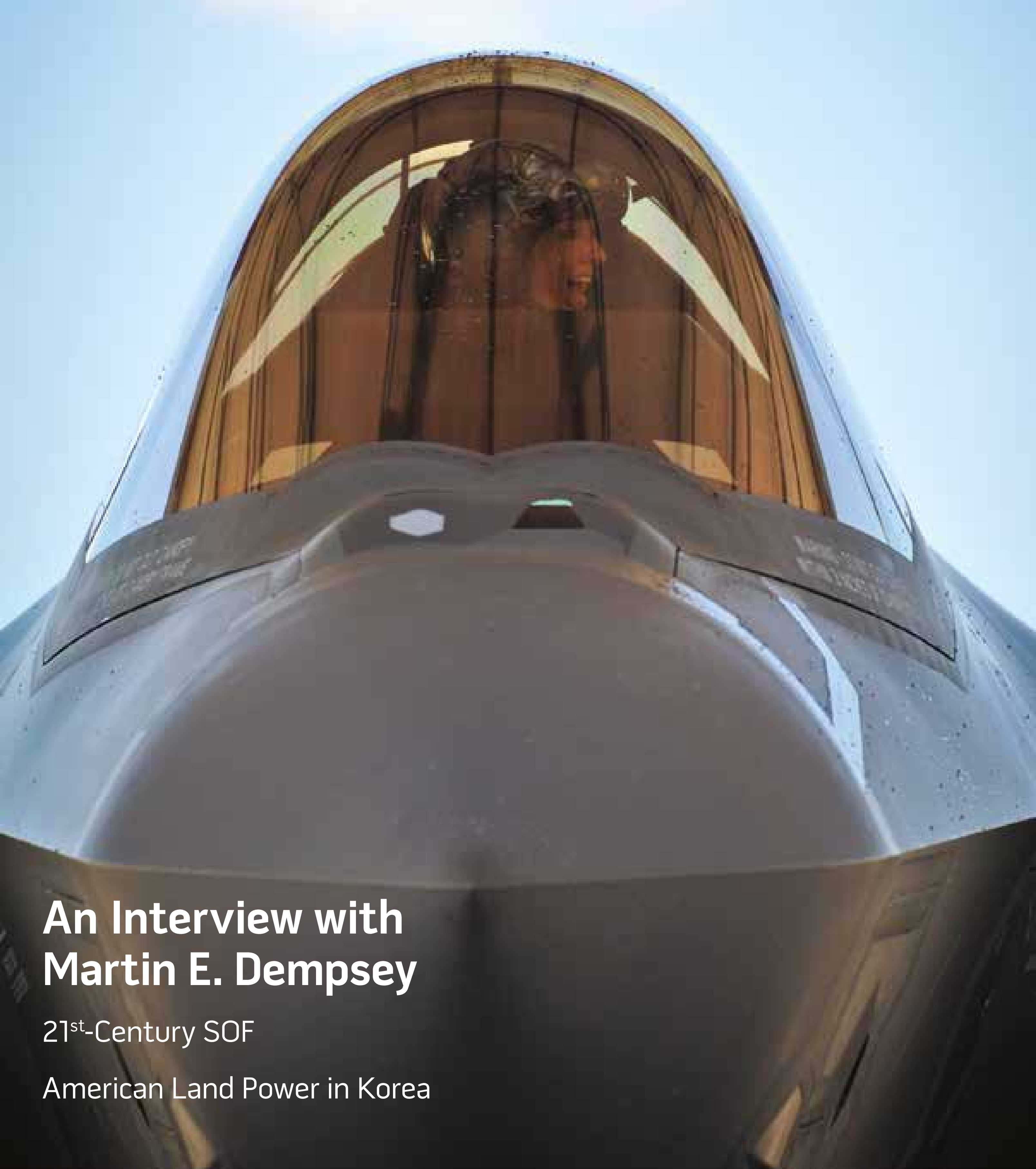
JFQ | Joint Force Quarterly

Issue 78, 3rd Quarter 2015



An Interview with Martin E. Dempsey

21st-Century SOF

American Land Power in Korea

Joint Force Quarterly

Founded in 1993 ▪ Vol. 78, 3rd Quarter 2015
http://ndupress.ndu.edu

GEN Martin E. Dempsey, USA, Publisher
MajGen Frederick M. Padilla, USMC, President, NDU

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

Executive Editor
Jeffrey D. Smotherman, Ph.D.

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

Internet Publications Editor
Joanna E. Seich

Copyeditor
Erin L. Sindle

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

Printed in St. Louis, Missouri, by UNIVERSAL Printing Company

Cover 2 images (top to bottom): U.S. Soldier assigned to Bravo Company, 1st Squadron, 9th Cavalry Regiment, 2nd Brigade Combat Team, 1st Calvary Division, provides security outside enemy compound during Decisive Action Rotation 15-05 at National Training Center, Fort Irwin, California (U.S. Army/Richard W. Jones, Jr.); U.S. Marines assigned to Force Reconnaissance Platoon, Maritime Raid Force, 26th Marine Expeditionary Unit, conduct HALO jump during category 3 sustainment training in Louisburg, North Carolina (U.S. Marine Corps/Andre Dakis); Chief Cryptologic Technician (Technical) Sailor assigned to amphibious dock landing ship USS *Pearl Harbor* hugs daughter after returning from 4-month deployment supporting Pacific Partnership 2013 (U.S. Navy/Todd C. Behrman)

In this Issue

JFQ Joint Force Quarterly
Issue 78, 3rd Quarter 2015
An Interview with Martin E. Dempsey
21st-Century SOF
American Land Power in Korea

About the Cover

Lieutenant Colonel Christine Mau, 33rd Operations Group deputy commander—notably first woman fighter pilot accepted into F-35 program—completes initial F-35A Lightning II training flight at Eglin Air Force Base, Florida, on May 5, 2015 (U.S. Air Force/Marleah Robertson)

Dialogue

Forum

JPME Today

Commentary

Features

Recall

Book Reviews

Joint Doctrine

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 by email to JFQ1@ndu.edu, with "Attention A&R Editor" in the subject line. 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: www.dtic.mil/doctrine/jfq/jfq.htm

3rd Quarter, July 2015
ISSN 1070-0692

U.S. Marine Corps M-198 155mm Howitzer gun crew of 4th Battalion, 14th Marines, Mike Battery, Gun 4, at Camp Fallujah engage enemy targets November 2004 (U.S. Marine Corps/Samantha L. Jones)

From the Chairman

An Interview with Martin E. Dempsey

On January 7, 2015, Dr. R.D. Hooker, Jr., Director of Research and Strategic Support at the National Defense University (NDU), and Dr. Joseph J. Collins, Director of the Center for Complex Operations in the Institute for National Strategic Studies, interviewed General Dempsey at NDU. Giorgio Rajao and Joanna E. Seich transcribed the interview.

Joseph J. Collins: Can you tell us how your views on the wars in Iraq and Afghanistan have evolved over your assignments as division commander, Multi-National Security Transition Command–Iraq [MNSTC-I] commander, acting U.S. Central Command commander, U.S. Army Training and Doctrine commander, Chief of Staff of the Army, and Chairman of the Joint Chiefs of Staff? That is an impressive set of perspectives on these wars.

General Martin E. Dempsey: I'd like to start with a vignette. I arrived in Iraq late June 2003 and took command of the 1st Armored Division. I had watched developments from Riyadh, where I was the program manager of the Saudi Arabian National Guard. There, I was being fed a pretty steady diet from my Saudi interlocutors about what was going well and what was not. I was also getting fed a heavy diet of Sunni Islam, obviously, and so I, like Bing Crosby, went on the road to Baghdad.

When I got to Baghdad, there was a sense of constant transition almost to the point of turmoil. For instance, I arrived just after Lieutenant General Dave McKiernan pulled out the CFLCC [Coalition Forces Land Component Command]. If you remember the CFLCC story, he was told, I wasn't in the room, but I was led to believe LTG McKiernan was told by Secretary [Donald] Rumsfeld to take as much risk going out as coming in, which sounds like something Secretary Rumsfeld would have said. So CFLCC had literally taken this command and control architecture, unplugged it, and went back to Kuwait in the process of redeploying. V Corps, as you recall, was left behind with General [Ricardo] "Rick" Sanchez. And my sense was that V Corps was little suited as a command and control headquarters, understaffed and under-resourced, fundamentally a tactical headquarters.

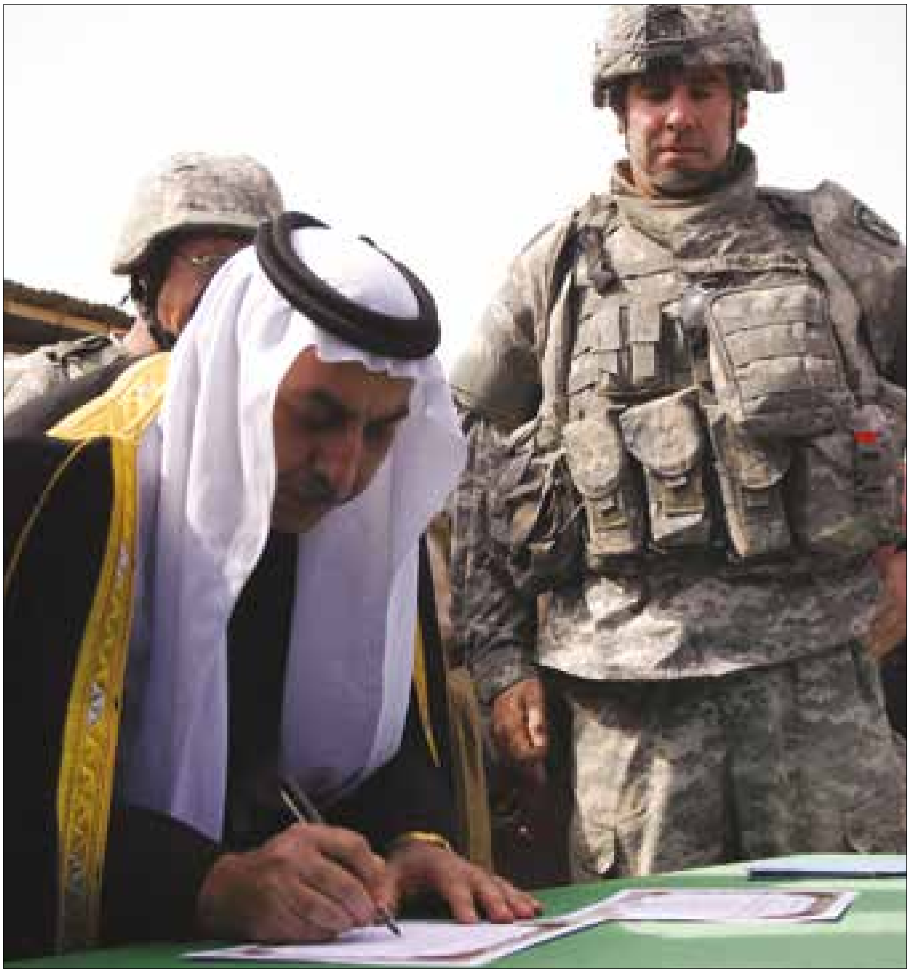
My sense was that we were a bit adrift frankly, at least in Baghdad. I can't speak to what was happening in Mosul, Ramadi, or Diyala Province. But in Baghdad, there was a bit of almost discovery learning, about what it means to have gone from this exquisite maneuver across the desert from Kuwait to Baghdad, to now being fundamentally responsible for the safety of a city of 7 million people, 75 square miles with a river running through it, and with deep ethnic and religious tensions.

I was trying to learn as quickly as possible what the mission was going to be because it was, quite frankly, unclear. The Iraqi army had been disbanded and de-Ba'athification had occurred. General David Petraeus at this time famously asked, "How does this thing end?" It was a fair question.

General John Abizaid came to see me around the time I took command, and I had a candid conversation with him about my initial observations, and I asked him as CENTCOM [U.S. Central Command] commander: "What is my mission, how would you articulate the intent?" And he replied, "Look, you're going to have to take this armored division, you're going to have to adapt it so that it can provide stability operations capability. . . . I don't have to tell you how to do that." But he added, "That's job number 1: how do you take this organization that you have and tailor it in order to provide a safe and secure environment in Baghdad?" I replied, "That's a pretty heavy lift, a safe and secure environment in Baghdad." He also asked, "How long do you think we have here?" I knew exactly what he [was thinking] because he's an Arabist; he'd been a scholar and an Arabic speaker. And I knew that he was asking whether the United States had a shelf-life here, or was this something we could consider doing in perpetuity, if necessary. From my experiences in Saudi Arabia, I answered, "Three years." He stated, "I think you're right."

General Dempsey (DOD)

That was in 2003. Since then, I have realized in a conflict that either creates or inherits a failed state—in a conflict where the issues are historical as opposed to topical, in a conflict where religion is a factor—you separate yourself from your adversaries by *innovation*, not necessarily by size and technology. The rate of innovation and adaptation is likely to be the most important quality of a military campaign, not the things we normally focus on, such as Force Management Level [FML]. It seems like a recent thing with this administration, but we have been debating FML from the very start with Secretary Rumsfeld. We debated and negotiated resources before we debated and negotiated objectives. That's my observation of my time between 2003 and the end of the Iraq War. You might place this observation on the negative side of the ledger, debating resources rather than objectives, but when objectives change,



Sheik Abdullah Sami Obeidi, a Sunni Arab tribal leader, signs declaration of support for Sons of Iraq program as U.S. Army Colonel David Paschel, commander of 1st Brigade Combat Team, 10th Mountain Division, looks on in Al Noor, Iraq, March 9, 2008 (DOD/Samuel Bendet)

we should simply recognize this and adapt accordingly. Sometimes changing objectives is portrayed as mission failure, when in fact in a protracted campaign the likelihood of renegotiating objectives is 100 percent.

On the positive side we were able to adapt. One could argue some were late to need, but the changes we made in intelligence gathering, assessment analysis, exploitation, and dissemination were important. When I visited a combat outpost on the Pakistani border in 2008 as the CENTCOM commander, Captain McChrystal, Stan's [Stanley McChrystal's] nephew, was in command. The captain had more access to national technical means and all kinds of intelligence in 2008 than I did as division commander in 2003, and that's not hyperbole. So we did make a lot of great adaptations to all of the battlefield functions, whether fires and maneuver or command and control, and we began to describe it as mission command. We decentralized, we began to empower the edge, and we began to develop the leaders who could work, seize, and execute initiatives. We began to improve intelligence functions and logistics. We learned a lot about contractors on the battlefield, some good and some bad. But we made a lot of incredible adjustments over time.

Let me finish by going back to the somewhat negative side. Architectures in organizations begin to develop a momentum of their own, and it becomes difficult to disassemble them. The architectures themselves become self-fulfilling. I didn't think we were ever going to get out of Baghdad with all of the architecture—intelligence, logistical, command and control—we had built there.

Moreover, we probably retained a little too much control for a little bit too long. We probably didn't make our relationship with former Iraqi Prime Minister [Nouri] al-Maliki as transactional and conditional as it should have been. As a result, we began, toward the end of the campaign, to be talking past one another. So that's kind of the front end and the back end.

On the MNSTC-I side, which is right in the middle for me from 2005 to 2007, I know some of your questions relate to a particular one: Can we actually build and develop indigenous forces to take control of their own country? Here is where I find myself today on this question. If we take ownership in every sense of the word, which we did in the early days both in Iraq and Afghanistan, and then try to begin to build an indigenous force in an institutional design to control it—that is to say not only tactical-level fighters but also the logistics architecture, intelligence architecture, school systems, and the ministries—that's far more difficult than making the indigenous force own it from the beginning with our enabling it.

So you might ask, what would you do differently. First of all, I would have absolutely not disbanded the Iraqi army, and I would have absolutely not de-Ba'athified. We lost all of the bureaucrats who knew how to run the country. And I would have, in a transactional and conditional way, made it clear how we would help the Iraqis regain control of their own country, put it back on its feet. But there would have been no doubt from the start that it would be their responsibility and not ours.

The enduring lesson about MNSTC-I is this: The art of campaigning and building a foreign military is establishing ownership and managing that from the start. If you take too much ownership too soon, it is almost impossible to give it back.

R.D. Hooker, Jr.: I interviewed a Combined Security Transition Command–Afghanistan deputy commander who believes that we tried too hard in both Iraq and Afghanistan to make those militaries like our own. Do you agree or disagree?

General Dempsey: I have thought about that a lot. Early on that was indeed a valid criticism. I remember going to visit Bernard Kerik, who was the senior Coalition Provincial Authority [CPA] police trainer. Kerik was passionate about not wanting the military involved in the training and only wanted occasional support with resupply as we conducted patrols in Baghdad, thus assuring the police stations were getting what they needed. He was training them to be beat cops, traffic circle cops, training them in law enforcement techniques. Then they graduated, went out into the streets of Baghdad, and were slaughtered.

Kerik left and the next guy that came in—I can't remember his name—I went to him and said, "Look, this can't be a competition, but I'm telling you the police you are producing are not going to stand and fight this insurgency because they're underarmed, they don't have protection around their stations, [and] they're getting slaughtered in the streets." So we forged a partnership. [Years later] I came back as commander of MNSTC-I. The next guy who came in was actually open-minded about having the police effort subordinated to MNSTC-I. It was on my watch that we gained oversight not only of the army but also of the police, and we were able to harmonize the efforts. But to your point, there's no question that early on we were trying to create these forces in our image. I don't regret that actually because we probably had to see if that was possible before we adapted.

We also had coalition partners that would take sectors of Iraq. The boon and bane of a coalition, as you know, is that it is a coalition—so everyone gets a voice. The boon is they're there, and you get 26, 28, or 45 flags. But there's no doubt in my mind, I can give you chapter and verse, that the way the British were developing the security forces in Basra was different than the Poles were developing security forces, and it was different than the way the [U.S.] Army was developing security forces in Diyala Province, different than the way the [U.S.] Marines were developing security forces in Al Anbar. Even in our own Service we had different approaches, a different way of partnering. Now is that a strength or a weakness? Initially it was a weakness because we were a little inconsistent. I think over time, however, we were able to harmonize that.

I remember visiting a country—I won't mention which country but it wasn't ours—and I went to its training center for the Iraqi security forces, and the trainers had a [significant amount of] instruction on drill and ceremonies. You see, the Iraqis loved to march—I mean they loved to march. But it wasn't doing them much good to keep them alive. But because they loved to march so much, and they were well behaved when marching, this particular partner was spending a lot of time teaching them how to march.

Hooker: Many sources, including the recent RAND study by Linda Robinson, have discussed the tension between civilian decisionmakers and their military advisors in making wartime decisions, particularly in the formation of objectives and the development of strategic options. What has been your experience, and what is your advice to pass on to successors?

General Dempsey: I think the system is actually designed to create that friction in decisionmaking. Our entire system is built on the premise that we require friction to move [forward]. Physics even says that. You have to have friction before the wheels on a car make contact with the road and propel it forward. So our system is designed to create a certain amount of friction, and it succeeds. There are always [institutional] equities, or the objectives as articulated by the Department of State and USAID [U.S. Agency for International Development]. One of the debates in Iraq early on was which comes first, economic development or security. It was a chicken-and-egg argument. Those were heated debates about whether we should lock down the country and then kind of loosen the reins on it and do economic development in a secure environment, or whether we should invest mightily into transitioning state-owned enterprises into private-owned enterprises. I can remember really serious, important, and constructive debates about that dichotomy. It was a false dichotomy, but it was presented as a dichotomy nonetheless.

First, I would advise future leaders that friction and disagreement in decisionmaking is not a negative. Frankly, you should embrace friction. What I found was, and I can't put a percentage on it, but in general the person at the table with the most persuasive argument tends to prevail in those environments.

Let me segue to an important factor. There is an article, I don't know who wrote it, but it was written in 2013, and it focuses on the uncanny ability of military and political leaders or elected officials to talk past each other. In the military culture, as you know, we spend decades learning how to do campaign planning, and we start with a well-stated and clear objective. Then we build a campaign to achieve that objective, with intermediate objectives and milestones along the way. Then we come up with three courses of action: high risk, medium risk, and low risk. We pick the middle-risk option and execute. If you are an elected official, the likelihood of your conceiving a well-crafted and well-defined objective at the beginning is almost zero. Rather, as an elected official, your first instinct is to seek to understand what options you have.

So militarily I know I've got it, I have a nuclear option, but let's just park that for a moment. What other options do I have in this magnificent toolbox called the U.S. military? What tools do I have that I can apply pressure with, that I can manage escalation with, and that I can integrate with the other instruments of national power? Elected officials are hardwired to ask for options first and then reverse-engineer objectives. And the military is hard-wired to do exactly the opposite.

Now what do we do about that situation? Nothing frankly. But that is the environment that we live and work in. I learned that pretty early on. I learned it by reading [Bob Woodward's] *Obama's Wars* [Simon & Schuster, 2011]. I read it not to get inside information on the intrigue or the kiss-and-tell aspect, but I wanted to try and understand why Woodward was able to find the seam between the advice that was given to the President and his willingness to accept that advice. And it came down to what I just described: it wasn't articulated that way in the book, but that's what I drew from the book. When you read a book, the author wants you to take what you want to take from it, and not necessarily what he is trying to give you. But I've decided that we're just hardwired differently. Knowing that, I think it's incumbent on us to work inside that culture and not to rebel against it. [This is a factor] in my relationship with the President, in my relationship with the JCS [Joint Chiefs of Staff], and it informs my relationship with the COCOMs [combatant commands] as I try to manage demand and supply. It has been quite helpful to me.

Getting back to the question, my advice to my successors is get to know how our government functions. Don't come to Washington thinking you're going to get Washington to conform to your beliefs because that is generally never going to happen. You have to have a moral compass, but you have to understand the way people in this city make decisions. Also, you must understand that most big decisions are made in conjunction with budget cycles, not in conjunction with current events. If you want to change something in our system of government, you change it in the budget. Can you do things in between budgets cycles? Of course you can; we built in a certain amount of flux, but big changes are [usually] made in budget cycles, and that includes big changes in campaigns.

Collins: If we could just follow up on that. You talked about the surge process in Afghanistan, and of course there was a surge process in Iraq. Any reflections on things that you have in your own personal knowledge or that you've learned from those particular cases in terms of decisionmaking?

General Dempsey: To thread that, or to link that back to the question about the RAND study and whether friction is a negative or a positive, the way that Multi-National Force–Iraq [MNF-I] was constructed was [that it would be led by] a strategic 4-star—[General] George Casey at the time, later David Petraeus—and two 3-stars. The two 3-stars were the Multi-National Corps–Iraq [MNC-I] commander, and me as the MNSTC-I commander. Both 3-stars had equal access and equal voice to the strategic command. MNC-I measured his success on levels of violence, but the MNSTC-I commander measured his success on the development of the Iraqi security forces. When the question of the surge came up, the advice of the MNC-I commander, not surprisingly, was that in order to drive down violence, he needed five brigades. (By the way, I may be off by a couple. Initially it was only two brigades, then eventually it went to five brigades.) And my advice was that we probably should knock violence down, but let's be careful on how we do it because we could give the Iraqis the idea that every time violence spikes, we would rush in and retake control of things. We could be actually setting back the development of the Iraqi security forces. Or, stated in another way, I said, "Look, we have two options here, General Casey. You can double down on [U.S.] activities and you will probably knock the violence down pretty quickly, or you can double down on the development of the Iraqi security forces. In other words, embed at greater numbers, enable at greater numbers, but actually make them responsible for pushing the surge and bringing the spike in violence down. And my advice is the latter: we have said that our exit strategy here runs through the Iraqi security forces. So if you want my advice as the MNSTC-I commander, I think we ought to double down on the Iraqis and not double down on ourselves."

That is exactly how the conversation went. Somehow along the way I've been painted with the brush of being anti-surge. I was never anti-surge. My question was simply who was going to surge. And my advice as the MNSTC-I commander was that the surge ought to be carried out by the Iraqis. It is debatable whether they could have pulled it off, but we had two separate 3-star commands in Iraq for that purpose. The decision was taken to dial down on our efforts, and I saluted, and we executed. Did it work? It did actually; it knocked the level of violence down, and the surge gave decision space for the Iraqi government, but it failed to take advantage of that space. One might make the case that they failed to take advantage because we had sent the message that if they get into trouble, we will rescue them. And I believe that, too; if you're trying to restore stability to a failed state, do you do it or do they do it? And the surge sent a signal that if something really went badly, we would take control of it, and then we would give them another chance. The other way to do it would have been violent; it would have taken longer. I'm not suggesting I was right and they were wrong, but I think I was there to give exactly that advice. And I gave it.

The other way of considering the surge as the right course of action is to look at the transactional and conditional nature of relationships, especially in that part of the world. What actually made the surge work? Again, this is debatable, but in my judgment, what made the surge work was less about the introduction of additional U.S. forces and more about the fact that we co-opted the Sunni tribes by paying them and arming them on the promise that the Iraqi government would absorb them into their security forces. Well, okay. It didn't happen. And because it didn't happen, the loyalty of the Sunni tribes went to us and not to the Iraqi government. Once we took the other decision to stop paying them and stop supporting them, and they didn't have a safety net in the Iraqi government, I think we are where we are today somewhat as a result of that. But that's controversial.

I do think the structure of MNF-I was designed so that the strategic command would get advice on both sides of the equation, which is how much should we do and how much should they do. It was my responsibility to argue for what they should do. I made the case, and the decision went the other way. History will decide if this was correct.

Collins: The other question was the Afghanistan surge. You touched on that with your mention of [Woodward's] *Obama's Wars*. In crafting options for those situations, should the most senior military people address all the options, or only the options they think are the ones that are going to work?

General Dempsey: The one thing that has to be clear: every option in military doctrine has to be suitable, feasible, and acceptable. I could never conceive of a circumstance where I would either recommend or, if asked, support an option that I didn't find to be feasible, acceptable, and suitable. But with that said, in particular because of what I've said earlier, I want to make sure this is not lost because I have been giving a lot of thought to this. In the use of the military instrument of power against state actors, we differentiate ourselves by size and technology. We are bigger, badder, our tanks shoot further, penetrate more deeply, and can operate at night in a way that our adversary cannot. So we overmatch with size and technology in state conflict. Training, good leadership, and [a] better logistics system—all of these are important.

When you talk about conflict against nonstate actors, and that is really what we are talking about here, we were fighting an insurgency on behalf of a government. We were fighting an insurgency on behalf of Iraq and an insurgency on behalf of Afghanistan, simultaneously trying to restore their abilities to govern. In that kind of conflict, the use of military [forces] against nonstate actors, I think size and technology matter, but what matters more is the rate at which we innovate. The rate of innovation becomes a better predictor of success than the Force Management Level, for example. Size matters, but the rate at which we can innovate, adapt, and respond to changes in the environment matters more.

In that context, this is where I answer your question. The options are far broader in conflicts with nonstate actors because decisions are temporal in a way. If I am right about the need to adapt more frequently, then the last thing we want to do is flop in there with 150,000 [personnel], 12 mega-forward operating bases, [and then] begin to funnel in TGI Friday's and Baskin-Robbins.

When I look back, conflict against nonstate actors does not lend itself to industrial-strength solutions. And I'm not sure exactly what I would have done differently, but I would have been far more expeditionary, far more austere, and far more attuned to the need to [innovate and adapt] than negotiating the Force Management Levels. For example, in Afghanistan we did surge, and that one ultimately may have had a better effect than the one in Iraq, but even in conducting that surge, we surged traditionally with BCTs [Brigade Combat Teams]. We took BCTs and surged for 12 consecutive cycles. By so doing, the industrial machine began to crank, and we started to build big FOBs [forward operating bases]—and big FOBs increase demand, demand increases requirement for money, et cetera. There is probably a way to redefine *surge*, but we looked at it through the lens of Force Management Levels. I wasn't in the system at the time. I was the TRADOC commander, but the President was told: "Look, it's 40,000 or nothing; 40,000 or let's get out." That is how it was portrayed. Is that right, though, is that really true, 40,000 or let's get out?

So we have to be a little less dogmatic in conflict against nonstate actors than we are in conflict with state actors. When we are in conflict with a state actor, it tends to be more existential, it tends to be a little clearer on how you differentiate yourself, and therefore I think the options become a little crisper. I don't find the options to be that crisp in this kind of conflict, and therefore we have to be more thoughtful and more open to negotiating them, remembering that we have to have a moral compass.

And by the way, I have one tenet that I generally rely on in making recommendations in places like Iraq and Afghanistan, and here it is: A squad's work for a squad. If you want me to do X, here is what I think I need to do. If you think I need to do it for less, then I am going to do less. My military advice is what you can accomplish with a squad, what can you accomplish with a battalion, what can you accomplish with a brigade, and we will not ask a brigade to do a division's worth of work. That is it, and we have had some success in discussions that are built on that principle.

Hooker: Historians are going to wrestle with whether the outcomes of the Iraq and Afghanistan campaigns were fundamentally ascribable to the military effort or civilian effort. There is a narrative that asserts the military was asked in both conflicts, at least once we got into the counterinsurgency game, to secure the population, and it did that fairly well. The military was able to build up large numbers of host nation military units that took over the transition. But the failure of the campaign was the inability of the host-nations, both in terms of the capacity and in terms of rule of law, to carry their loads. That was the vulnerability we were never able to overcome. Do you see it that way?

General Dempsey: Remember earlier when I said that in conflict against nonstate actors in failed states or failing states, I have come to believe that support needs to be transactional and conditional. I believe that because, generally speaking, in these failing and failed states the issues are societal—they are not political issues. Sometimes they begin as political issues, or they'll start as representational—for instance, the fruit vendor in Tunisia self-immolating because the government wanted to tax his fruit stand. It starts political, but it goes pretty quickly to sectarian issues, to religion, and ethnicity because these are historic impulses that have been suppressed for generations. In those environments, it's absolutely predictable that the "victor and vanquished" mentality will quickly come forward. Those who have been suppressed will see themselves as victors, and they will come and vanquish those oppressing them, and I think whether we are asked to conduct military operations in Iraq, Afghanistan, Libya, Syria, [or] Nigeria, that "victor-vanquished" instinct is the dominant societal instinct. If I'm right about this, then there can be no unconditional support, in my opinion, because unconditional support will simply reinforce the "victor-vanquished" paradigm as it emerges.

So let's fast-forward to Iraq today. Some people are saying, "Why aren't you doing more, and sooner?" Our support needs to *remain as* support and *not* ownership. Furthermore, support needs to be conditional. If the Iraqi government does not meet its commitments to create a more inclusive political environment and to address some of the grievances of the Sunni and Kurd populations, then nothing we do will last. It will be painting over rust. We have eight lines of effort, two of which are military, and generally the military lines of effort leap out in front—and I do mean leap. That is who we are, right? If it is worth doing, it is worth overdoing. The military lines of effort will always be achieved. And that can be detrimental to the other lines of effort. I don't know if that answers your question, but it is why I believe now that the use of the military instrument of power in issues of nonstate actors and failed states needs to be far more conditional and transactional than anything we do with state actors.

One more thing: [U.S. interests must lead.] The tragedy of human suffering and the situation in Syria is awful, but I will also tell you the use of the U.S. military instrument of power without consideration of what I just described can actually create more harm and even further suffering, I think.

Collins: We have also had some grand failures in intelligence, in particular in the war in Iraq. One criticism, that in particular of General Michael Flynn, is that we are here fighting among people and we do not know much about them, and intelligence is not focused on that problem. How do you see intelligence functioning and its level of proficiency both operationally and strategically in Iraq and Afghanistan?

General Dempsey: The Intelligence Community was slow in adapting to what really mattered in the environments we found ourselves in. Back to the difference in state actors and nonstate actors: if I'm right about the fact that you differentiate yourself in a state conflict by size and technology, then the intelligence architecture is going to build itself in such a way to determine where capabilities are placing you at a disadvantage. In an environment with nonstate actors, where it is all about innovation, then you have to understand the factors that would cause you to need to innovate, and they largely reside in societal factors. You try to drive the insurgency or the terrorist group from the population. Mike [Flynn] was right; we could list the deck of cards or the wiring diagram of any number of organizations and networks in Iraq and Afghanistan, but if we were to ask a commander on the ground in Afghanistan to tell us something about this particular tribe in this particular valley and who are its affiliates, that was often discovery learning. Every time we had to RIP [relief in place] out a unit, it was discovery learning again, so we fell into a bit of the 12 1-year campaigns instead of one 12-year campaign. Mike's article actually helped a lot with that, and we had done some things with TRADOC, with the HTTs [Human Terrain Teams], not without controversy by the way.

My TRADOC G2, a guy named Maxie McFarland, who passed away recently, was instrumental in developing and fielding the HTTs. It was his brainchild to reach out to academia, to anthropology, to form these teams and to offer them to BCTs. We would try to keep them there so the HTT would stay in the last 6 months of a brigade, and the first 6 months of a new brigade, so there was continuity. And they paid big dividends. We got this, and it was controversial still, because of the notion that we were perverting science, using science to the detriment of culture rather than to the benefit of it. But it was addressing the question you asked: how do you learn about the environment? And that is one answer.

This is in the spirit of learning lessons and not throwing stones. It took a while for the Intelligence Community to adapt to help us—that is to say the tactical commander to understand the environments—but there was progress. Now the question is whether can we sustain it. Or is the institution likely to forget that the understanding of culture, religion, and economics of a local society is important? I hope not, and with all the chiefs we seem to be committed to making sure that we don't forget those lessons, but often the institution will. It is like a rubber band; you stretch it and then you let it go, and it will go back to its normal form or shape. I'm afraid some of that might occur, if we are not careful.

My successor will face state and nonstate challenges in about equal measures. One thing Jim Baker [Principal Deputy Director, Strategic Plans and Policy, J5] helped me think through [is] the meaning of the reemergence of Russia. I was feeling kind of constrained by Russia, and the President asked me, "Can I meet my [North Atlantic Treaty Organization] Article 5 responsibilities?" And I replied, "Mr. President, that is a great question, so let me get back to you." I was feeling uncomfortable about the ability of our forces to use forward basing because in the last 10 years the Russians have developed some capabilities that actually could coerce and constrain us.

Jim pointed out that the world looked similar to that of the early years of my career. And there was truth in that. During the first 15 years of my career, 1974 to 1989, Russia was a near-peer competitor, not just nuclear but also conventionally. We were constrained, and our military planning took into account the fact that we were constrained in military operations by a near-peer competitor. We didn't like it, but we learned how to deal with it. The next 20 years, 1989 to 2009, had no constraints. So most of the officer corps today lived in a world where they were unconstrained. No one could prevent them from doing anything they wanted to do. But guess what? We are back to what is probably normal, I think, in the course of recent events—that is, to where you have near-peer competitors in

F/A-18C Hornet assigned to "Blue Diamonds" of Strike Fighter Squadron VFA-146 launches from USS *Ronald Reagan* to conduct close-air support missions in June 2011 as part of Operation *Enduring Freedom* (U.S. Navy/Alexander Tidd)

certain domains, and then you have to account for this in military planning.

So my successor will have to deal with the reality of state actors who can now coerce and constrain us, as well as nonstate actors. So, to your point, I don't think the pendulum will swing entirely back to Russia or China as peer competitors, but I think the institution will have to adapt to have aspects of both in them.

Hooker: How should future senior officers who are combatant commanders or the Chairman view their role in the highest councils of government? Are they there to provide the best military advice only, or are they there, as Clausewitz noted, to be both the statesman and general?

General Dempsey: When you become a senior military leader, you have multiple responsibilities, one of which is to give the best military advice possible, and another is to help the force. But there is a third one, too. I have the responsibility to contribute to foreign relations strategy as a statutory advisor of the National Security Council. In my early days, we would go around the room, and the staff would be talking about something I didn't want to talk about. Pick a topic. Whatever it was, as it came around the room for me, I would say, "I am here as your military advisor; that is not a military issue." And the President would say, "Yes, but you are here, and I want your view on this strategic issue that has national security implications."

If you are going to understand how decisions are made in our government, you must build relationships, and if you're going to build relationships, you have to demonstrate a certain gravitas. You've got to be able to have a conversation about grand strategy, not just military strategy. If I had to give advice to my successors about job number one in terms of being influential inside decisionmaking boardrooms, it would be that relationships matter most of all. If you can't develop a relationship of trust and credibility—credibility first and trust second, because trust is earned—then you won't be successful in contributing to our national security strategy.

Collins: You come down almost exactly at the same point JFK did after the Bay of Pigs. He wrote instructions to the Joint Chiefs that said very much what you just said in the last 2 or 3 minutes. We have had a number of issues having to do with detainees' enhanced interrogation. Some of those shoes have not dropped yet for the Department of Defense, military commissions, and so forth. Were these problems inevitable, or did we get off on the wrong foot? If 10 years from now we have another situation akin to the situations in Afghanistan and Iraq, what would you tell your successor about the lessons and how we did it in these two cases?

General Dempsey: The detention operations have to be included in any campaign

B-1B Lancer aircraft drop six GBU-38 munitions onto insurgent torture house and prison in Northern Zambraniyah, Iraq, March 2008 (U.S. Air Force/Andy Dunaway)

plan that includes the use of military force because we can't ever put a young man or woman in the position where there's no possibility of detention. The alternative is capture and release, or kill not capture.

I think this is what happened in these conflicts regarding detention operations. You know what they say about campaign assumptions: if the assumptions are flawed or invalid, the campaign has to be adapted. That's why you make assumptions about campaigns. So one of the assumptions I think we made, again I was in Riyadh when all this was being developed, but I think one of the campaign assumptions, probably driven more by political aspirations than the reality, was that [we would] go into Iraq and we would be welcomed because we would be seen as liberators, and we could take as much risk getting out as we took getting in. One of the risks we took going in was that we went in with fewer forces than the commander thought he needed to accomplish the task. Fewer forces mean fewer capabilities. We didn't have the number of MPs [military police] that we probably needed to account for detention operations because we didn't think that we'd be detaining enemy personnel. Or if we were detaining, we would be turning them over to I don't know whom, but the assumptions were flawed. So yes, we got off on the wrong foot, but we also hadn't done detainee operations since 1991.

But if you remember in 1991, the 96 Hour War, I can remember as part of VII Corps accumulating large numbers of Iraqi soldiers surrendering, and we pulled them down into Saudi Arabia into temporary camps. But I think we repatriated them within weeks, not months. And so if you go back to the time before when we did detainee operations, you have to go all the way back to Vietnam, so there was a lot of rust on that function. If there is a lesson here, it's the lesson that comes to us instinctively, which is to address the worst-case scenario. We always do that, but we're talked out of it sometimes, and I think in the case of detainee operations in future conflict, we shouldn't allow ourselves to get talked out of that function.

Collins: Are enhanced interrogation techniques a bigger issue for the Central Intelligence Agency or the Department of Defense?

General Dempsey: Our issue was an initial lack of doctrine. Then we had the terrible incident in Abu Ghraib, and then the Army republished its doctrine and from that point forward, we had no further problems.

So linking it back to your last question, the key here is to continue to refresh our doctrine in order to manage the functional area. As we shrink the force, we have to be careful not to eliminate that capability. A lesson of this conflict will be that leaders need to be involved. Again, I was in Baghdad, and the only thing I controlled in Abu Ghraib was external security, but I'm pretty sure I'm correct in saying that we just turned it over to the MPs to manage without proper oversight. So leadership matters whether you're talking about combat operations, detention operations, or intelligence operations. Remember, I described that scenario in June 2003 when we actually didn't settle in on a definition of the enemy, an organizational principle to design against it, and a campaign that acknowledged that this was going to take some time. Even in August 2003 we were talking about the possibility of being home by Christmas. So we didn't grasp the fact that this was going to be a protracted campaign until October. So think about the time between March and October—that's 6 months. So there's a 6-month period of indecision there, and that's where some of these bad habits, worse than bad habits, this misconduct began to manifest itself. There was a list of enhanced interrogation techniques, but Abu Ghraib was clearly not a problem of enhanced interrogation—it was misconduct.

Collins: General [Daniel P.] Bolger states clearly that the wars in Iraq and Afghanistan have been lost. In fact, that is the title of his book [*Why We Lost: A General's Inside Account of the Iraq and Afghanistan Wars* (Houghton Mifflin Harcourt, 2014)]. And senior military leaders bear much of the responsibility. He suggests that we should have left Afghanistan and Iraq somewhere within the first 6 months. Would such a thing have been possible?

General Dempsey: No, that's not who we are as a nation. I wish things were that simple. Imagine being able to just go in and crush that which you can find, declare that you've accomplished your task, and care nothing about what you leave in your wake and withdraw. But that's not the American way of war, not to sound too much like Russell Weigley [Distinguished University Professor of History at Temple University and noted military historian], but that's not the American way of war. The American way of war tends to be that—out of a sense of not only obligation and responsibility to protect, although that is not really doctrine, but also compassion—we assist those who have been defeated to reestablish themselves in a more moderate and inclusive way. As far as whether we made mistakes, I take no exception to that, but I consider it more about learning than about negligence. And I think as we learned, we changed. Now to Bolger's point about whether we stayed there too long, 6 months certainly was not possible. If he would have said in the book that we should have had an idea as to how long we were willing to make this commitment from the start and that should have informed our thinking about how to organize the campaign, I accept that, but 6 months is absurd.

Hooker: Can you compare your experience working for three different Secretaries of Defense? Do you have any thoughts on varying styles of civil-military negotiations from one to the other?

General Dempsey: All *very* different. As Chief of Staff of the Army and at CENTCOM, I had the opportunity to work with Secretary [Robert] Gates. So really I've had some close relationships with Gates, [Leon] Panetta, [Chuck] Hagel, and [Ash] Carter. First of all, I don't think I've changed who I am to adapt to them, but I have adapted the way I interact with them and that's probably an important distinction. I'll give you some examples.

Secretary Gates was a voracious reader and a very close reader. You could give him a read-ahead document and you could expect that when you engage with him, he would have some close and crisp questions. He let the written word inform him, and so when you engaged with him one on one or in a meeting, it tended to start at a higher level.

Secretary Panetta was a man of uncanny instinct. Even before reading something or discussing it, he had been around so long and had had so many experiences inside of government—whether in the White House as Chief of Staff, in Congress, or as the Director of the CIA—that he learned less by reading and more by interacting. He also believed deeply in relationships. So if you were able to forge a relationship with him and you gained his trust, it made the interactions extraordinarily collegial.

So going from one to the other—understanding that the written word was important—I focused a lot on, especially when I was at CENTCOM, I wrote my own weekly reports, organized them and selected [the precise] words, and I managed the length of report in a way that I knew would match Secretary Gates's way of learning. With Secretary Panetta, I'm not sure; I may have given him maybe three documents in 18 months or in 2 years. In any case, he probably knew what I was writing before I wrote it, and what he really wanted was to engage me on it. So we had a very close relationship built mostly around the time we spent in his office.

Secretary Hagel also comes from a background of long government service, whether it was as President of the USO, Deputy Director of the VA [Veteran's Administration], an academic at Georgetown University, the Senate, and Secretary of Defense. He has […] a greater instinct not for detail but for the theory of the case. He likes to understand not only the tactical question, but also how that question fits into a broader frame. If Secretary Panetta was the quintessential extrovert, Secretary Hagel was kind of the quintessential introvert. That doesn't mean he's without humor. He's pleasant, he's engaging, he's compassionate, and extraordinarily connected to soldiers. Not only soldiers [but also] the lower ranking enlisted [of all the Services] expressed their deep disappointment that he's leaving. Somehow he actually found a way to make a connection with the sergeants, petty officers, Airmen, and ensigns that was quite remarkable. He is one of them. He doesn't care for detail, and he doesn't care for big groups, whereas with Panetta, you couldn't put enough people in the room for him because he could just own it, honestly. He was a remarkable facilitator of huge audiences. Secretary Hagel was much more comfortable with smaller groups. He also likes to read, and so he's kind of a hybrid of Gates and Panetta. Secretary Hagel is a one-on-one guy. He does his best thinking, his best work, and his best interaction one on one. So back to the question. I think I'm still the same person I was 3 years ago, but I'm a little savvier. I've adapted the way I interact with these leaders based on the way they learn, and you have to figure that out.

Collins: In our crowdsourcing of strategic lessons of the wars, a number of folks are saying that when we look back through history on a grand scale, foreign expeditionary forces in counterinsurgency operations are successful only in rare circumstances. The British were successful in Malaya, but then again the British were the government, so there was no sanctuary. The United States was successful in the Philippines in 1902, but again it was the government, and again there was no sanctuary. But other than those two cases, many experts claim that this cannot be done. We have now been involved in Iraq, Afghanistan, and Vietnam. How should your successors think about this in the future? Is this the sort of mission we have to still prepare for, or is this something that is beyond the pale?

General Dempsey: If you mean by "beyond the pale" large-scale intervention against nonstate actors or insurgents and failing states, let me use Iraq as an example.

Today, I'm at bat for the third time in Iraq. I was literally in Iraq sitting on what we later called Route Tampa in the aftermath of the 96 Hour War, blocking that major highway that runs from Kuwait to Baghdad. I sat there for a couple of months. You remember the debate about whether we should have pursued the Republican Guard and end the event right then and there, or whether we should have settled for the narrowly defined objectives in the [United Nations] Security Council resolutions and so forth.

The 96 Hour War accomplished the objectives, and as a result, we ended up leaving for the first time in the central region a large force that was there both as a deterrent and a reassurance for our allies. Prior to 1991, we had a permanent naval base in Bahrain, but I don't think we had a permanent land base (we may have had access to some air bases). We weren't in Qatar and we weren't in [the United Arab Emirates]. One might argue that although the Gulf War looks to have been a lot cleaner, it did result in a requirement to place a pretty significant footprint there that has put a strain on the force ever since.

Then we go from 2003 to 2011, and I think we've wrung that out as much as we can, but here's what I think is different this time when we talk about our reentry into Iraq. I think we've got it about right, which is to say, we've made it clear that we will support and enable, that we'll keep the eight lines of effort apace, even if some of them will get a little ahead of each other on occasion. But we're not going to take ownership of Iraq again. And I think that we can accomplish this task with a light footprint and the use of some of our key enablers, but we've got to have resolve and courage. If the government of Iraq proves to be incapable or unwilling, we've got to be willing to dial it back. In other words, it has to be conditional; it just can't be unconditional in this kind of environment because we have other options to deal with the terrorist threat, but Iraq doesn't have any other options to deal with this insurgent threat.

I would like to tell you that large-scale intervention during insurgencies will be a thing of the past, but we have to retain the capability. That's why we've established building partner capacity as a core competence of the entire force, not just special operators. Security force assistance as part of theater campaign plans is prominent in the Phase 0 side of operations, but I don't think we should size the force to counterinsurgency; we should size the force for treaty obligations against state actors and then retain enough slack in the system so that we can ensure readiness.

We're getting ready to enter a huge debate about the correct balance of forward stationing, rotational deployments, and readiness of standing forces. Right now, the model we have produces readiness and deploys contingent upon combatant commander demand signals. That's especially true in the Air Force, the Navy somewhat, pretty much true in the Marine Corps, and except for a handful of brigades, pretty much true in the Army. So we have everything distributed globally, but if there were some major contingency or if there were something that would surprise us that would exceed the capacity of a particular COCOM to deal with it, the only place to get forces and readiness would be from some other COCOM. There's almost nothing stationed in CONUS [the continental United States] that is unused capability or readiness, so we've got to go back and address that.

Prior to 1991, we were a lot bigger—781,000 in the Army alone. We would have a fraction of the force forward deployed, and we would have these big Reforger exercises, for example. The forces would be stationed mostly inside CONUS, and the idea was that these forces would be at various degrees of readiness, but more or less ready in CONUS for deployment into contingency operations and the forward presence part of it wasn't the priority. The priority was the readiness part of it.

Since 1991, the paradigm's reversed. The priority now is forward presence to include rotational presence, thereafter security cooperation, Phase 0, Phase 1—that's the priority now. Phase 3, combat, we're taking risk, frankly, because we've got much less than we probably should have in readiness in CONUS.

I'm not suggesting we're going to flip it again. Some would argue that we should flip the paradigm back to where we prioritize surge capacity and readiness as the primary effort. I don't think we'll do that, but I think you'll see us try to rebalance it.

The part of the force that tends to be forward is the part that is most capable of doing the kind of things you're talking about in terms of counterinsurgency, counterterrorism, building partner capacity, and so forth. As we change the paradigm, we have to figure out a way to make sure that the training that supports the new paradigm accounts for both maneuver warfare and low-intensity conflict.

I think my successor will probably have to refresh the military lexicon a bit. You said before that Bolger said, "We lost Iraq and Afghanistan." This statement implies we didn't win in Iraq and Afghanistan. Yet one of my premises is that the definition [of winning] is frequently redefined in [the current] environment. Saying categorically "win" or "lose" seems to be far less applicable to those kinds of conflicts than it is in a high-intensity conflict with a peer competitor that is trying either to take your territory or deny your freedom of movement.

Hooker: Is it a mistake to think in terms of war termination, or are we in the middle of an ongoing conflict, maybe less than a war, but a conflict that is unlikely to end anytime soon and that we ought to adapt to?

General Dempsey: You remember back in the early part of the last decade the phrase "the Long War." That phrase attracted antibodies of all kinds [. . .] fiscal antibodies, political antibodies, and intellectual antibodies. Then George Casey kind of led the charge on use of the phrase "persistent conflict." And his view, if you don't want to concede that this is actually a war in the strictest or loosest definition of the word, you should at least accept the fact that we're going to be in persistent conflict. Of course, eventually that fizzled as well. I don't remember exactly why that one fizzled, but it hasn't actually been replaced. If we have indeed ended the wars in Iraq and Afghanistan, what do we have? We still have Soldiers and Sailors and Marines deploying in harm's way. If you're a pilot flying over Iraq, the distinction between combat advising and no boots on the ground is meaningless.

We've had some success, but there's work to be done on acknowledging and understanding what runs from Western Pakistan to Nigeria: a group of organizations that sometimes work with each other and sometimes operate independently, depending on their objectives, that are trying to take advantage of lack of governance almost everywhere, that are playing to this victimization psychology, and that use the tactics of terror. And there is a fine line here: are these people terrorists, or are these people using the tactics of terror? What we've discussed, both inside the military and with the administration and Congress, is that this threat [. . .] of violent extremist organizations—most of which also happen to be radical Islamic organizations—we as a nation just haven't had a conversation about that. I've been accused of being anti-Islam by some and pro-Islam by others. I guess in that sense I'm succeeding in managing the conversation. But the point is there are violent extremist organizations that are using a religious ideology to brand themselves and to gain support from disenfranchised populations, both Sunni and Shia.

As long as this conflict persists, every 10 years or so a new generation will be sucked in. And until this cycle is broken—and that cycle is likely not to be broken exclusively and not even primarily with military force—the despair, lack of hope, lack of inclusive governance, and grotesque economic disparity will continue, and the U.S. military will be called upon to have a role in addressing it.

How we define that role is to be determined. Right now, we're defining it one country and one group at a time. In fact, if you look at the way our country plans are written for the counterterrorism, if you look at the way the State Department organizes itself and interacts with us, interacts with the combatant commanders, it is one group, one country at a time. But it's a common threat. We have not successfully helped our elected officials address this threat in its totality, and until we do and until we can actually find the right vocabulary, I think we will continue to be effective at containing the threat and to the greatest extent possible and keeping it from our shores, but we will not be effective at ultimately defeating the threat until we capture the right framework, which is actually transregional, and until we capture the right vocabulary. That's not to suggest, by the way, I think that absolutely the wrong thing would be to agree that it's transregional and find the right vocabulary, and then decide that we're going to invest enormous military resources to stabilize all of these countries and put them back on a firm footing for their future. Because that won't happen. They will allow us to do that—you know many of them will. We'll be embraced initially, then disdained and attacked ultimately by the very people that we think we're helping.

You asked a great question right at the beginning of this interview about the future of counterinsurgency. Is it possible to build an indigenous force that will actually take control of its own destiny? I don't know. But I think that's the path to addressing that challenge in the future. In my judgment, the wrong answer is for elected officials to ask me the question they often ask, which is, "What are *we* [the U.S. military] going to do about it?" I get that all the time: "What are you going to do about Syria?" Here's my response: "I'm going to try my best to find a way to integrate the military instrument of power with the other instruments of government and look for our diplomats to form coalitions and find a political path that we can enable with the use of military power." **JFQ**

General Dempsey on UH-60 Blackhawk helicopter while flying over Kabul, February 2012 (DOD/D. Myles Cullen)

Executive Summary

Every so often we find ourselves in a place where we can take time to assess where we are, where we have been, and where we think we are going—and check it against where we think we should be ending up. This edition of *JFQ* offers two interviews that are assessments of events past, present, and future. Both are of stories not yet complete: one, the wars in Afghanistan and Iraq; the other, the production of the F-35 fighter aircraft. The first of these interviews is with the 18th Chairman of the Joint Chiefs of Staff General Martin Dempsey on his views about the wars in Iraq and Afghanistan, the decisions that were made that shaped these wars, and their outcomes. General Dempsey provides a candid assessment of what he experienced both "in country" as well as his interaction with his superiors at different times over the past decade and more. He also offers some important insights about civilian-military relationships that he knows from firsthand experience. Consider this a must-read for those who may find themselves in this "arena" at the top of the executive branch. The second interview is with Lieutenant General Christopher Bogdan, USAF, who is the Program Executive Officer for the F-35. Lieutenant General Bogdan provides his views on where the F-35 is headed while addressing the "stories of the past." Both interviews will in many ways surprise you as well as let you hear from the officers who are best positioned to see the time horizon of a nation's wars and the place for the machines we build to fight them.

In our Forum section we bring you a broad range of important security issues that will take you from the halls of the Pentagon to the Arctic. William Patterson provides a timely review of the rise of Islamic terrorism in Kenya, where hundreds have been killed and wounded in recent years due to various attacks by groups, including al-Shabaab. Returning *JFQ* author Kevin Stringer sees the Arctic as the place joint special operations forces should focus on in the years ahead. Stephen Watts, J. Michael Polich, and Derek Eaton, graduates of the Joint Forces Staff College, discuss how the Department of Defense can focus its efforts to rapidly regenerate our irregular warfare capacity given the withdrawals of major troop deployments from Iraq and Afghanistan in recent years.

A lineup of some of the most experienced instructors from around the military academic community fills our roster in this issue's JPME Today section. The U.S. Army War College's Charles Allen discusses how his college goes about educating senior military officers in leadership and creative thinking. From Newport and the Naval War College's Distance Education Department, George H. Baker, Jr., and Jason E. Wallis present an interesting take on ethical decisionmaking that offers a useful new tool for faculty and students alike. At the U.S. Army Command and General Staff College, Dale Eikmeier is uniquely positioned to reflect on wargaming at the operational and tactical levels of war.

In Commentary, as a well-known professor of strategic leadership at the Naval War College (and a fellow press director), Carnes Lord offers his views on the relationship between military professionals and civilian leadership.

Our Features section brings a range of issues including cyber, ballistic missile defense, land power in Asia, and North Atlantic Treaty Organization (NATO) training. G. Alexander Crowther and Shaheen Ghori lead off with a discussion concerning what U.S. Government cyber activity looks like and how to interpret that view. Andrea Little Limbago helps us think about how cyber statecraft works. Another team from the Joint Forces Staff College, Thomas K. Hensley, Lloyd P. Caviness, Stephanie Vaughn, and Christopher Morton, explains what is involved in providing adequate warning for our ballistic missile defenses. Land power in Asia has become an important discussion item alongside the more publicized Air-Sea Battle debate. Lieutenant General John "JD" Johnson and Bradley T. Gericke remind us that land power is still central to a successful outcome in any future crisis on the Korean Peninsula. From NATO, John G. Norris and James K. Dunivan give us a much-needed look inside the Alliance's efforts to keep land forces trained, integrated, and ready to respond through the efforts of NATO's Joint Military Training Center in Germany.

F-35B Lightning II takes off from USS *Wasp* during routine daylight operations (U.S. Marine Corps/Anne K. Henry)

The National War College's Mark Clodfelter, one of the Nation's leading scholars on strategy and the application of airpower, brings us back to Vietnam in this issue's Recall article. Our Joint Doctrine section contains a thought-provoking piece on center of gravity analysis as it applies to the current fight against the Islamic State of Iraq and the Levant, and includes an updated list of recently revised joint publications. We also present three book reviews that we hope you will enjoy.

Whether you agree with what our authors and the generals we interviewed said, I want you to know that you can take a position on these and any other issues. You *should* take a position. Argue with your teammates. Wrestle with what is happening today and what is likely to happen tomorrow. Not everything we publish here should be taken at face value. These are the ideas of the authors and in many cases they do not align with their organizations' points of view. *JFQ* offers you that opportunity to say what you think matters. Got a better view? Write it up and send it to us. We have thousands of people looking for you to have a say. That's how the joint force will remain the best in the world. Or at least that is how I see where we are going. **JFQ**

William T. Eliason
Editor in Chief

Garissa Market in Nairobi suburb Eastleigh (Dan Kori/Wikipedia)

Islamic Radicalization in Kenya

By William R. Patterson

In September 2013, an attack carried out by the al Qaeda–affiliated terrorist group al-Shabaab on the Westgate shopping mall in Nairobi, Kenya, drew renewed attention to the extremist threat facing that country. At least four attackers left more than 65 people dead after a multiday rampage. All four of the known assailants were Somalis who had been living in the Nairobi suburb of Eastleigh, known for its large Somali ex-patriot population. Four other Somalis have been charged with helping to plan the operation, two of whom had Kenyan citizenship and identification cards.[1] This attack was only the latest in a string of terrorist incidents stretching back to the late 1990s. It should serve as a stark reminder to the United States that terrorism remains a significant threat to its national interests in Kenya specifically and in the Horn of Africa more generally.

The first major terrorist attack to hit Kenya occurred at the U.S. Embassy in Nairobi on August 7, 1998. This attack was carried out with a truck bomb, killing 214 people and injuring more than 5,000. On November 22, 2002, another set of attacks included the detonation of a truck bomb at an Israeli-owned resort and the launching of missiles at an Israeli-chartered aircraft leaving the airport in Mombasa. Sixteen Israelis and Kenyans were killed in the blast at the hotel, though no one was killed in the attack on

Dr. William R. Patterson is a former Social Scientist with the Human Terrain System who served in Afghanistan and has been selected to be a Foreign Service Officer with the Department of State. This article is a modified version that the author originally published while serving with the Human Terrain System.

the plane. Al Qaeda was responsible for each of these attacks.[2]

Since those early attacks, the government of Kenya has become an important strategic partner in the U.S. Government's counterterrorism efforts in the broader Horn of Africa region. In October 2011, the Kenyan Defense Forces launched an offensive against al-Shabaab called Operation *Linda Nchi* (OLN)—Swahili for "protect the nation"—in Somalia. While OLN enjoyed the approval of most Kenyans, it also prompted criticism from Kenyan Muslim communities.

In 2012, Kenya passed a tough antiterrorism bill called the Prevention of Terrorism Act 2012. Though the passage of this bill was not as controversial as some earlier iterations, it still elicited criticism from Kenyan human rights and Muslim groups. In addition, riots blaming the Kenyan police for the extrajudicial killing of al-Shabaab–linked Muslim Youth Center (MYC) cleric Aboud Rogo[3] and the growing activity of the MYC are indicative of increased Islamic radicalism in Kenya. This presents a substantial risk of terrorism against the Kenyan government, Western targets in Kenya, and neighboring countries in the region.

This article explores the development of radicalization in Kenya in recent decades and the sociocultural and political factors that have undergirded it. Additionally, it highlights four general factors influencing the rising threat of Islamic radicalism in Kenya: institutional weaknesses; increasingly acute grievances by the Muslim minority; the establishment of Wahhabi and other extremist forms of Islam in Kenya, along with attendant jihadi ideology and propaganda; and Kenya's foreign and military policy, particularly as it pertains to Somalia.

Islam in Kenya

Approximately 4.3 million Muslims comprise a little more than 10 percent of the overall Kenyan population and about 30 percent of the coastal population.[4] Large concentrations of Kenyan Muslims live in Coast Province, North East Province, and the capital city of Nairobi, particularly in the neighborhood of Eastleigh. Ethnically, Kenya's Muslims are primarily Swahili or Somali, although there are also sizable Arab and Asian (predominantly Indian and Pakistani) groups.[5]

In addition to ethnic divisions among Kenya's Muslims, there are also key differences in the types of Islam practiced. Scholar Bjørn Møller writes that the Kenyan Muslim community can be categorized as follows:

- a majority of indigenous Kenyan Muslims belong to Sufi orders, especially in rural areas
- reformists, more conservative Islamists, are another primary grouping, mainly in the cities and among Arabs
- a small sect called the Ahmadiya, which was responsible for the first translation of the Koran into Kiswahili, probably numbers no more than a few thousand
- mainstream Sunni Muslims, mainly among Asians
- a small number of Shi'ites, also mainly among Asians.[6]

Muslims settled on Pate Island (part of the Lamu archipelago in Coast Province) as early as the 8th century. This presence grew considerably during the 12th century as trade increased in the Indian Ocean in general and along the coast of East Africa in particular. The earliest Muslim settlers came primarily from what are now Oman, Yemen, and Iran, establishing communities along the Somali coast, Lamu, Mombasa, Zanzibar, and other coastal areas of East Africa.

As these settlers intermarried with each other and with local people, Swahili culture evolved over time. Islam became the core of Swahili culture, but the culture was also influenced by many traditional aspects of indigenous African religious beliefs.[7] Lamu and Mombasa became the primary areas of Islamic learning and scholarship in Kenya.[8] Swahili culture and Islam remained largely confined to the coastal areas where trade flourished, though Islam eventually established a foothold in the capital city of Nairobi as well.[9] Among some of the settlers, particularly in Lamu, were *sayyid*s, descendants of the Prophet Mohammad.[10] Traditionally granted great authority within the Muslim community, that authority came to be challenged during the 20th century and remains an area of contention between different Muslim groups today.

During the end of the 19th and beginning of the 20th centuries, the territories that make up Kenya today were colonized by the British Empire. The interior of the country was chartered to the Imperial British East Africa Company in 1888, became a formal protectorate in 1895, and a colony in 1920. The Muslim coastal area remained a protectorate but was administered in the same fashion as was the colony, meaning there was little practical difference.[11]

Administratively, the British categorized people as either native or nonnative, providing different privileges to each, with nonnative receiving preferential treatment. Swahilis did not fit easily into either of those categories. As Jeremy Prestholdt points out, "most occupied the awkward position of having neither a recognized African 'tribal' identity nor the higher legal status of Non-Native. By the end of the colonial era, this nebulous position contributed to perceptions of Swahilis as neither completely African nor, by extension, Kenyan."[12] The legacy of that division remains today as many contemporary Kenyans continue to see Muslims more as foreigners than as true Kenyans.

Another colonial practice that served to split Muslims from the larger society was the introduction and special treatment of Christianity. Abdalla Bujra explains that Christianity came to predominate in Kenya, and Western culture generally developed preeminence through the school system and through examples set by colonial officials and British settlers. Kenya's Muslims became culturally isolated as the Christian Church and Western educational system became established in the rest of the country.[13] Not only was Christianity privileged, but Islam was also denigrated. Bujra notes that "through Church activities and education, and later through the colonial education and media, both Church, Colonial Administration, and the European settler communities propagated very strong anti-Arab and anti-Islamic misinformation and propaganda. Hence Swahili/Arab political influences essentially came to a halt in [Kenya]."[14] This political disenfranchisement has never been remedied and remains a major grievance of Kenya's Muslims to this day.

The political disenfranchisement of Kenya's Muslims continued after Kenya's independence in 1963. The Kenyan African National Union (KANU) immediately came to power and instituted one-party rule. KANU, strongly linked to Christian ethnic groups, was perceived as benefiting those groups disproportionately while largely ignoring problems specific to Muslims.[15] Due to their marginalization in the political process and consequential lack of influence in Kenyan politics, dissent grew among Muslims. Immediately upon Kenyan independence, the Mwambao United Front movement emerged in Kenya's coastal communities calling for the autonomy of the coastal strip of Kenya. This was seen by some Kenyan Muslims as the only way to achieve a political system that honored their religious beliefs.[16] Today the Mombasa Republican Council has taken up this cause and has attracted significant support.

Other Swahilis attempted to use the more traditional political route by establishing the Islamic Party of Kenya (IPK) in 1992. However, explicitly religious parties are illegal in Kenya, and the IPK was denied formal political participation. The IPK complained that all existent Kenyan political parties are, if not in name at least in fact, Christian oriented and led by Christians.[17] The rejection of the IPK as a legitimate political party has been perceived by many Muslims as another form of political alienation and as a deliberate suppression of Muslims' ability to express their views through the political process.

In addition, many of Kenya's Muslims perceived themselves as being excluded from employment opportunities available to other Kenyans. This was especially the case as Kenyans from the interior of the country began to buy property along the coast during the burgeoning tourist industry. Seeing little opportunity for themselves in Kenya, many Muslims traveled abroad to the Middle East, particularly Saudi Arabia, for work. Authors Esha Faki Mwinyihaji and Frederick O. Wanyama note that:

> *The employment sector was seen as closed to many Muslims. As a result of the oil boom in the 1970s and 1980s, many young Muslims went to work as expatriates in Saudi Arabia where the remuneration was good with the minimal education they had. For almost two decades Saudi Arabia and the Persian Gulf served as a safe haven for some Kenyan Muslims to work and progress economically.*[18]

One of the impacts of greater exposure to the Middle East—and Saudi Arabia in particular—was the introduction of stricter interpretations of Islam by Kenyan Muslims returning home. This provoked a conflict between older Swahili interpretations of Islam that incorporated elements of indigenous African religions and practices imported from the Middle East. This schism was also generated by Kenyan students who completed their studies in the Middle East. In so doing, they adopted stricter religious practices, which they brought back with them to their communities.[19] According to Kai Kresse:

> *Proficient in Arabic, the graduates returned with university degrees and the reformist doctrines of their respective host institutions, which were more radical and combative in tone and content. They applied these ideas to the East African context in their teachings and public speeches, thus radicalizing reformist discourse and polarizing Islamic debate more and more.*[20]

An individual named Sheikh Muhammed Khasim was especially influential along the Swahili coast.[21] Khasim was most active during the 1960s and 1970s and argued that traditional Swahili Islam included impermissible *bid'a* (innovation in religious matters) and *shirk* (violating the principle of the unity of God) due to the influences of indigenous religions.[22] He sought to purify Kenyan Islam and to eliminate the power of the sayyid (also called *masharifu*), whose power base remained centered in Lamu. Kresse explains that the conflict between Khasim and the masharifu

> *centered on the social and religious status of the masharifu, the descendants of Prophet Muhammad. In popular perception the masharifu, as holy persons with special blessings, fulfilled an important religious function of mediating between Muslim commoners and God, via the Prophet Muhammad, to whom they were said to be especially close. But Sheikh Muhammed Khasim insisted, with reference to the Qur'an, that they did not have any such special powers and, furthermore, it was up to each individual to establish a direct contact to God through special prayers (dua), independently.*[23]

Khasim distributed his teachings through pamphlets and educational books. This served to threaten the authority of the masharifu and represented an opening salvo in the dispute between Islam as traditionally practiced in Kenya and stricter interpretations of Islam more recently imported from the Middle East.

An illustrative case study of this rift is provided by Susan Beckerleg in her anthropological work in the coastal city of Watamu. A reformist movement called Halali Sunna took root there, which stood in opposition to the traditional masharifu. The adherents of this movement followed a stricter form of Islam and criticized the power of the masharifu as well as the indigenous elements that had long been established in their form of Islam. They also stressed participation in traditional Islamic observances such as prayer and the duty to imitate the life of Mohammed. The men grew their beards and wore traditional Islamic garb and the women also dressed more conservatively than did the typical Muslim women of Watamu. This sect was highly influenced by the conservative Tabligh Islamic movement, which originated in India in the early 20th century and which reached Watamu in 1990 by way of migrants.[24] The adherents of this movement were also evangelical and worked vigorously to spread their ideas.[25]

Much of the local impetus for this reversion to a more conservative form of Islam sprang from social changes being imposed on the community by outside pressures. As Watamu became a popular tourist destination for Westerners, the young people of Watamu became increasingly exposed to the use of alcohol and drugs; immodest dress at the beach, especially by women; and other behaviors that contradicted traditional Islamic precepts and rules of behavior. The adoption of a stricter interpretation of Islam was one way to push back against these disorienting cultural and social changes.[26] This phenomenon was not limited to Watamu and was in fact occurring in Muslim communities in popular tourist destinations throughout coastal Kenya in particular.

This push for the adoption of a more conservative "pure" form of Islam, as opposed to the more traditional form of Islam influenced by indigenous African religion, created a space for the development of radicalization in Kenya. The reform movement can in retrospect be seen as a first step toward a more radicalized and militant form of Islam establishing roots in the country. The rift created between traditional and reform Islam became more adversarial over time, especially as outside actors, most prominently from the Middle East and South Asia, began to increasingly influence the movement. Kresse writes that:

> *Differences in practice and understanding of Islam, which were once tolerated, turned to spark off strong animosities, and the intellectual center of reformist ideology shifted from an internal to an external position, as a multitude of Islamic groups from around the world have sought to increase their influence and support.*[27]

The trend toward radicalization catalyzed by the reform movement soon combined with other forces and only grew stronger during the 1990s and 2000s.

Smoke rises above Westgate Mall in Nairobi, September 23, 2013 (Anne Knight/Wikipedia)

Forces of Radicalization

There are four main factors that have served to intensify the country's vulnerability to radicalization and terrorism: structural and institutional factors, grievances, foreign and military policy, and jihadist ideology.

Structural and Institutional Factors. There are several structural and institutional factors that make Kenya vulnerable to radicalization:

- the relatively advanced economy and infrastructure allows for freedom of movement and an abundance of targets
- weak governance in key areas such as security, criminal justice system, and rule of law impede effective action against terrorist groups[28]
- geographical proximity to unstable states, particularly Somalia, in conjunction with porous borders.[29]

Economy and Infrastructure. It seems counterintuitive that a relatively robust economy and infrastructural system—compared to neighboring countries—would make Kenya vulnerable. But as Raymond Muhula puts it, "Kenya's attractiveness to terrorists is exacerbated by the fact that it also boasts the best infrastructural facilities in the region. It is far easier to operate a cell in Kenya than in any of the Horn countries."[30] Radical and terrorist groups require resources to thrive. Infrastructure and some degree of economic stability allow for ease of travel, faster communications, and access to resources.

In terms of communications, Mwinyihaji and Wanyama point to the Internet as being particularly important:

> *Rapid internet diffusion has led to a mushrooming of cyber-cafes charging users less than a dollar per hour. These units have become crucial sites of Kenyan Muslims' engagement with the global Muslim ummah, enhancing their knowledge of Islam through cyber-literacy, and networking within and between (cyber)-communities with shared interests.*[31]

Such communication is much more difficult to achieve in a failed state such as Somalia.

The infrastructure also offers enticing targets for terrorist groups. Airports, hotels, resorts, restaurants, and nightclubs, as well as government buildings such as the U.S. Embassy, are easily accessible to terrorists. Furthermore, tourists themselves are possible targets either while they are in the country or during their transit to and from, as the 2002 attacks on the Israeli hotel and charter plane demonstrate.

Weak Governance. Weak governance, especially in critical areas such as criminal justice, border security, and the provision of essential services, also increases Kenya's vulnerability to radicalism and terror. Widespread corruption, unguarded borders, and ineffective security and police organizations allow terrorist organizations freedom of movement, the establishment of safe havens, and the ability to coordinate logistical needs.[32]

A weak criminal justice system can also result in impunity for terrorists. When suspects are caught, they are frequently able to evade justice through bribery or as a result of sheer incompetence in the system. This weakness not only allows terror suspects to unjustly go free but also fosters police abuses due to their inability to use the legal system successfully.

Geography. Kenya's close proximity to unstable states (Somalia, Uganda, South Sudan, and Ethiopia), along with its inability to protect its borders, are other risk factors. This is especially true of Somalia and even more so in the aftermath of Operation *Linda Nchi*. The al-Shabaab terrorist group in Somalia sends adherents back and forth across the border.[33] Additionally, Kenya's proximity to the Arabian Peninsula, Egypt, and the Middle East more broadly has allowed for the steady penetration of jihadist ideologies as travel between Kenya and these areas is relatively easy.

Grievances. Kenyan Muslims have several grievances, many of which have their roots in colonial history. The structural and institutional vulnerabilities discussed above exacerbate these grievances:

- lack of representation in politics
- discrimination and lack of economic, educational, and other opportunities
- heavy-handedness and human rights abuses by the police and antiterrorism legislation and tactics.

Political Representation. Since Kenya's independence from Britain in 1963, the country's Muslims have been politically marginalized. For most of this period the KANU held power in a one-party system. However, even after Kenyan politics became more democratic, the interests of the Muslim minority have been largely ignored in political circles.

The government established an official Muslim organization—the Supreme Council of Muslims of Kenya (SUPKEM)—in 1973. It was the only organization authorized to represent all of Kenya's Muslims, and SUPKEM leaders were closely allied with the political establishment.[34] Being a tool of the government, however, many Muslims viewed it more as a way to control them than to meet their unique interests. The organization was not seen as useful for expressing any political ideas, opinions, or needs that were not already acceptable to the government.

The situation has marginally improved since the end of one-party rule. There are now several national-level Muslim entities with some degree of independent political influence. These include, among others, the National Muslim Leaders Forum, Majlis Ulamaa Kenya, Kenya Council of Imams and Ulamaas, and Council of Imams and Preachers of Kenya.[35] These are primarily interest groups and councils, however, and do not wield any direct power or authority. While they give the Muslim community an outlet to express itself, they have not led to sufficient representation within government itself or to remedies for the unique problems and interests of Kenya's Muslim communities.

Without political power, Muslims have not been able to advocate successfully for the needs of their communities and have largely been left behind in terms of economic and educational opportunities. Lacking a legitimate political path to address grievances, some Muslims turn to religious extremism to affect change. A report prepared by the United Nations Monitoring Group responsible for East Africa noted that:

> *During a 13 September 2010 lecture, addressing* [Muslim Youth Center, an offshoot of al-Shabaab] *combatants and other Swahili-speaking fighters in Somalia, Ahmad Iman dissuaded Kenyan Muslims from engaging in national politics, urging them instead to "Chinja" (cut), "Chonga" (peel) and "Fiyeka" (slash) the throats of the* [Kenyan] *infidels and "to hit back and cause blasts* [in Kenya]" *similar to the Kampala bombings.*[36]

Alienation from legitimate political institutions may continue to increase the appeal of violent attacks.

Discrimination and Lack of Opportunity. Lack of opportunity, in some cases as the result of discriminatory policies, contributes to widely held grievances in coastal Muslim communities. Fathima Badurdeen argues:

> *The root cause of youth radicalization in Coast stems from the region's desperate economic, social, and political conditions. Ineffective decentralization of development plans and governance issues since independence form the backbone of this situation, which is taken advantage of by an infrastructure of social networks or religious and political groups that provide communities with what the government does not and are in some instances extremist.*[37]

Unemployment is rife in the Muslim population. North East Province, Nairobi, and Coast Province, all three with high Muslim populations, had the highest levels of unemployment in the country as of 2005–2006,[38] as well as the highest rates of youth unemployment in 2008.[39] Furthermore, economic development in the tourism industry, particularly in Coast Province, has generally advanced without input from the local Muslim population and has also largely excluded them from its benefits. Fatima Azmiya Badurdeen writes, "The government's attitude toward and plans for the coastal communities have led citizens in Coast to feel that their resources are being used for the benefit of others."[40] She provides the example of a port development project in Lamu. Locals believed that the project was being forced on them and complained that they have had little input regarding decisionmaking. This lack of local representation is typical of the types of interactions that have led to high levels of resentment.

Disparities in educational opportunities have also been a problem, and with less access to government-run schools, many Muslim families have turned to madrassas and to foreign education. According to the International Crisis Group (ICG), since the late 1970s Kenya's madrassas have been dominated by wealthy Wahhabi charities and foundations. Madrassas at the primary and secondary level have been prevalent throughout urban areas for decades and have frequently focused on teaching Arabic and Wahhabi theology. In fact, religious inculcation rather than an employable education has often been the primary aim of these institutions. The brightest of the students would then be granted scholarships to Wahhabi-oriented universities in Saudi Arabia, Pakistan, or other Middle Eastern countries.[41]

Finally, many Kenyan Muslims also say they are discriminated against by the government overall. They complain of being treated as foreigners, about the inability to get documents such as IDs and passports, and harassment of citizens from Arab countries coming to Kenya.[42] This has been particularly difficult since the strict enforcement of passport regulations implemented in 2001. After the terrorist attacks of 9/11, the United States pressured the Kenyan government to more scrupulously examine the passports of citizens of Asian or Arab descent. In response, the government has required that to obtain a new passport or renew a previously held one, citizens of Asian or Arab ancestry, including Swahilis, must present their grandfather's birth certificate—a requirement that few Kenyans of any group can comply with. Many Kenyan Muslims consider the enforcement of these restrictive passport laws to be openly discriminatory against them "at the behest of the United States."[43] As seen below, many grievances held by Kenyan Muslims stem from such counterterrorism efforts.

Counterterrorism and Human Rights Abuses. The bombing of the U.S. Embassy in Nairobi in 1998, the attacks on New York City and the Pentagon in 2001, and the attacks against an Israeli-owned hotel and charter plane in Mombasa in 2002 brought terrorism to the forefront in Kenya. The United States pressured the government to enact various legislation and policies to fight terrorism in Kenya to prevent the country's use as a base for al Qaeda or other radical groups. However, some of these efforts have had the unintended consequence of further radicalizing elements of the population. Since the terrorist attacks in 2002, some Kenyan Muslims have complained of being unfairly targeted and of being the victims of human rights abuses, including arbitrary arrest and torture during interrogations.[44]

Muslim human rights groups operating in Kenya document government abuse. Al-Amin Kimathi, chair of the Muslim Human Rights Forum, claimed in media accounts that at least seven Muslims, most with alleged ties to al-Shabaab, disappeared in 2013. He also surmised that inefficiencies within the criminal justice system had hampered legal investigations and caused security officers to act outside of the law. According to Kimathi, "They [police] reach a point where they get frustrated by the law and the court process and they have realized that the only way to deal with these people is to 'disappear' them."[45]

Additionally, various legislative initiatives, particularly the Suppression of Terrorism Bill first introduced in 2002, have been viewed by many Kenyan Muslims as specifically targeting them. The bill was drafted with little or no input from the Muslim community, and it was criticized for having an overly broad definition of terrorism, extensive police powers to detain people, and providing the minister for internal security with the power to label any group as a terrorist organization. The most controversial aspect, however, was the power granted to police to arrest any person "who, in a public place wears an item of clothing . . . in such a way or in such circumstances as to arouse suspicion that he is a member or supporter of a declared terrorist organization."[46] Muslims feared that this would allow members of their community to be targeted merely because of their appearance. Due to these complaints, the bill was withdrawn. It was reintroduced in 2006, only to be defeated again.

In October 2012, the Prevention of Terrorism Act was passed. This law prescribes stiff punishments for people engaged in terrorist attacks, planning, recruiting, or other activities. It also allows terrorism suspects to be extradited to other countries for prosecution. Most of the issues that Muslims objected to in earlier versions of the bill have been ameliorated through amendments and this version garnered some support in the Muslim community.[47] Other Muslims continue to complain about the bill, however, again arguing that it is aimed at them.[48]

It is important to view these legislative initiatives and alleged human rights abuses in the context of social separation that has historically existed between Muslims and the government. Jeremy Prestholdt points out that "counterterrorism has alienated Muslim communities who for nearly three decades have voiced feelings of economic and political marginalization."[49] These counterterrorism actions, or the perceptions that they have created, have had the unintended consequence of exacerbating preexisting grievances and social cleavages. They have deepened an attitude of mistrust and have possibly had the opposite of their desired effect by further radicalizing aggrieved segments of the population. The International Crisis Group argues that while the threat posed by groups such as al-Shabaab is real, overreaction and human rights abuses by police and other security actors may be counterproductive. The group warns that "reckless police action has become a deepening concern and could radicalize Kenyan Somalis, as well as Muslims in general. Kenya urgently needs to reform its internal security services; what is presently on display is an incoherent system that weakens national security."[50]

Kenya has taken several steps to strengthen terrorism legislation, investigate terrorist organizations operating in Kenya, and arrest suspected terrorist operatives. These steps are crucial to inhibiting the ability of terrorist groups to operate there. They may backfire, however, if they are viewed as targeting the entire Muslim community or as relying on draconian tactics contrary to human rights. The unintended second-order effects of these efforts may be to increase radicalization and receptivity to the messages being propagated by terrorist groups. Closer engagement between government representatives and Muslim leaders over pending legislation, even-handed application of the law, and thorough investigations of alleged human rights violations may ameliorate some of these effects.

Jihadist Ideology. Jihadist organizations in Kenya use a variety of ideological tools and radical Islamic teachings to galvanize the Muslim population there toward violence. The grievances, cultural ties, and influx of jihadist philosophy through the increase of madrassas in Kenya have served to legitimate and spread radical ideology. Ethnic heritage is also an important factor. A report prepared for the Combating Terrorism Center at West Point notes that "Many residents of Mombasa, Malindi, and Lamu [all in Coast Province] hold stronger ties with the Arabian Peninsula than with Kenya's own interior."[51] Raymond Muhula also argues that ethnic ties make some of Kenya's Muslims particularly receptive to jihadist ideology emanating from the Middle East and other parts of the world.[52]

As noted earlier, over the past several decades there has been a reformist movement that has sought to "purify" Islam of the indigenous elements that it has accrued from traditional African religious practices. This movement led to the establishment of a more conservative—and eventually radical—form of Islam in Kenya. Radical jihadist ideology has been increasingly disseminated through mosques, madrassas, and community development initiatives[53] as well as through the radical publication *Al-Misbah*, which is published by the MYC and *The Weekly Muslim News Update*. Both of these publications have used Koranic teachings to foment jihad and have criticized the Kenyan government over a variety of issues including economic disparities and discrimination, arbitrary arrests, and Kenya's military relationship with the United States.[54]

Foreign and Military Policies. Kenyan foreign and military policies anger many Kenyan Muslims and serve as a powerful ideological tool for radicalization. They complain that the government's relationships with the United States and Israel are too close and that Kenya's multiple military interventions in Somalia targeted Muslims at the behest of the United States. The Islamic Liberation Army of the People of Kenya, for example, used Kenya's close ties with the United States and Israel as justification for the attack on the U.S. Embassy in Nairobi in 1998. After the attack they released the following statement:

> *The Americans humiliate our people, they occupy the Arabian peninsula, they extract our riches, they impose a blockade and, besides, they support the Jews of Israel, our worse* [sic] *enemies, who occupy the Al-Aqsa mosque. . . . The attack was justified because the government of Kenya recognized that the Americans had used the country's territory to fight against its Moslem neighbors, in particular Somalia. Besides, Kenya cooperated with Israel. In this country one finds the most anti-Islamic Jewish centers in all East Africa. It is from Kenya that the Americans supported the separatist war in Southern Sudan, pursued by John Garang's fighters.*[55]

Intervention in Somalia has been a particularly strong catalyst for radicalism among some Muslims in Kenya. In 2006, for example, the Kenyan government allowed the United States to use its territory to support Ethiopian military operations against Somalia. The government also cooperated with U.S. efforts to track al Qaeda operatives among the resultant refugees, and Kenyan security forces arrested at least 150 people from various countries. At least 90 of those arrested were later sent to Somalia and Ethiopia. The government denied that any of the deported refugees were Kenyan citizens, but Raila Odinga, an opposition candidate for the presidency, released the names of 19 Kenyan Muslims who he claimed were deported. This incident inflamed tensions with the Muslim community in Kenya and aroused their deep-seated distrust toward the government and heightened their sense of victimization.[56]

More recently, Operation *Linda Nchi* has led to protests and outright violence in Kenya. In October 2011, the Kenyan Defense Forces joined Somali, Ethiopian, and French troops in an operation to drive al Qaeda–affiliate al-Shabaab from Somalia. That intervention led to a backlash of attacks in Kenya itself. More than 20 attacks linked to al-Shabaab have been conducted in Kenya since the operation began. Most of these attacks have targeted nightclubs, bars, and churches.[57] The ICG warned at the time that:

> *Views within the ethnic Somali and wider Muslim community regarding the war are mixed but predominately critical. . . . The notion that the war is popular within the Muslim community is wishful thinking, and has the potential to exacerbate already worrying radicalization in the country is very real.*[58]

This turned out to be prescient.

Several historical and current factors have recently combined to increase the potential of terrorist activity in Kenya. Structural and institutional weaknesses, historical grievances, the influx of radical ideology, and military intervention in Somalia have galvanized extremists and increased the likelihood of terrorist acts in Kenya. Kenyan counterterrorism efforts will continue, but attention should be paid to their unintended second-order effects, as well as the historical and social context of these activities, so that negative effects can be ameliorated.

Islam is on a track of increasing radicalization in the country and groups linked to al Qaeda and al-Shabaab pose a significant and growing threat to Kenya and to Western persons and interests in that country. Recognition of the threat and its underlying causes is necessary for redressing those causes and reducing the threat level posed by radical Islamic groups. JFQ

Notes

[1] Lateef Mungin, "Hearing Starts, Adjourned for 4 Suspects in Kenya Mall Attack,"

CNN.com, January 14, 2014, available at <www.cnn.com/2014/01/15/world/africa/kenya-mall-trial/>.

[2] Johnnie Carson, "Kenya: The Struggle against Terrorism," in *Battling Terrorism in the Horn* of Africa, ed. Robert I. Rotberg (Cambridge, MA: World Peace Foundation, 2005), 180–181.

[3] Tom Odula, "Aboud Rogo, Kenya Muslim Cleric, Shot Dead," Associated Press, September 17, 2012.

[4] Jodi Vittori, Kristin Bremer, and Pasquale Vittori, "Islam in Tanzania and Kenya: Ally or Threat in the War on Terror?" *Studies in Conflict and Terrorism* 32, no. 12 (December 2009), 1084.

[5] Bjørn Møller, "Political Islam in Kenya," DIIS Working Paper No. 2006/22, Danish Institute for International Studies, 2006, 11.

[6] Ibid.

[7] Abdalla Bujra, "Islam in Eastern Africa: Historical Legacy and Contemporary Challenges," Development Policy Management Forum, August 2002, 6.

[8] Ibid., 7.

[9] Ibid., 11.

[10] B.G. Martin, "Islam in Lamu," review of *The Sacred Meadows: A Structural Analysis of Religious Symbolism in an East African Town*, by Abdul Hamid M. el-Zein, *Journal of African History* 17, no. 3 (1976), 453.

[11] Møller.

[12] Jeremy Prestholdt, "Kenya, the United States, and Counterterrorism," *Africa Today* 57, no. 4 (Summer 2011), 6.

[13] Bujra, 11–12.

[14] Ibid., 8.

[15] Jeffrey Haynes, "Islam and Democracy in East Africa," *Democratization* 13, no. 3, (September 2012), 497.

[16] Esha Faki Mwinyihaji and Frederick O. Wanyama, "The Media, Terrorism, and Political Mobilization of Muslims in Kenya," *The Politics and Religion Journal—Serbian Edition*, no. 1 (2011), 103.

[17] Vittori, Bremer, and Vittori, 1083.

[18] Mwinyihaji and Wanyama, 106.

[19] Kai Kresse, "Swahili Enlightenment? East African Reformist Discourse at the Turning Point: The Example of Sheikh Muhammad Kasim Mazrui," *Journal of Religion in Africa* 33, no. 3 (2003), 281.

[20] Ibid., 282.

[21] Ibid., 285.

[22] Ibid., 286.

[23] Ibid., 283.

[24] Susan Beckerleg, "'Brown Sugar' or Friday Prayers: Youth Choices and Community Building in Coastal Kenya," *African Affairs* 94, no. 374 (January 1995), 32.

[25] Ibid., 33.

[26] Ibid., 37.

[27] Kresse, 280.

[28] Clint Watts, Jacob Shapiro, and Vaid Brown, *Al-Qaida's (Mis)Adventures in the Horn of Africa* (West Point, NY: Combating Terrorism Center, July 2007), 47, available at <www.ctc.usma.edu/posts/al-qaidas-misadventures-in-the-horn-of-africa>.

[29] Ibid., 50

[30] Raymond Muhula, "Kenya and the Global War on Terrorism: Searching for a New Role in a New War," in *Africa and the War on Terrorism*, ed. John Davis (Burlington, VT: Ashgate, 2007), 47.

[31] Mwinyihaji and Wanyama, 105.

[32] William Rosenau, "Al-Qaida Recruitment Trends in Kenya and Tanzania," *Studies in Conflict and Terrorism* 28 (2005), 1.

[33] International Crisis Group (ICG), "Kenyan Somali Islamist Radicalisation," Africa Briefing No. 85, January 25, 2012, 1.

[34] Vittori, Bremer, and Vittori, 1083.

[35] Mwinyihaji and Wanyama, 104.

[36] United Nations Security Council, S/2011/433, "Report of the Monitoring Group on Somalia and Eritrea Pursuant to Security Council Resolution 1916 (2010)," 144, available at <www.un.org/ga/search/view_doc.asp?symbol=S/2011/433>.

[37] Fatima Azmiya Badurdeen, "Youth Radicalization in the Coast Province of Kenya," *Africa Peace and Conflict Journal* 5, no. 1 (2012), 54.

[38] World Bank, "Kenya—Poverty and Inequality Assessment: Executive Summary and Synthesis Report," 2009, available at <https://openknowledge.worldbank.org/handle/10986/3081>.

[39] World Bank, "Kenya Poverty and Inequality Assessment: Volume I: Synthesis Report," Poverty Reduction and Economic Management Unit, Africa Region, Report No. 44190-KE, June 2008.

[40] Badurdeen, 54–55.

[41] ICG, "Kenyan Somali Islamist Radicalisation," 11.

[42] Bujra, 16.

[43] Prestholdt, 9.

[44] Jeremy Lind and Jude Howell, "Counter-terrorism and the Politics of Aid: Civil Society Responses in Kenya," *Development and Change* 42, no. 2 (2010), 342.

[45] Clar Ni Chonghaile, "Kenyan Muslims Fear the Worst Over Proposals to Boost Police Powers," *Guardian*, September 27, 2012.

[46] Jan Bachmann and Jana Hönke, "'Peace and Security' as Counterterrorism? The Political Effects of Liberal Interventions in Kenya," *African Affairs* 109, no. 434 (2009), 108.

[47] Standard on Sunday Team, "Kibaki Signs Historic Anti-terrorism Bill," *Standard Digital News*, October 14, 2012, available at <www.standardmedia.co.ke/article/2000068354/kibaki-signs-historic-anti-terrorism-bill>.

[48] Wambui Ndonga, "Kenya: Kibaki Assents to Prevention of Terrorism Act," *AllAfrica.com*, October 13, 2012.

[49] Prestholdt, 5.

[50] ICG, "The Kenyan Military Intervention in Somalia," Africa Report No. 184, February 15, 2012, 8.

[51] Watts, Shapiro, and Brown, 51.

[52] Muhula, 47.

[53] Badurdeen, 56.

[54] Mwinyihaji and Wanyama, 107.

[55] Quoted in Haynes, 499.

[56] Bachmann and Hönke, 108–109.

[57] ICG, "The Kenyan Military Intervention in Somalia," 8.

[58] Ibid., 14.

Secretary Kerry listens as Arctic Council Chairman Leona Aglukkaq of Canada relinquishes council chairmanship to the United States during meeting of its eight member nations and seven Permanent Representatives, April 2015 (State Department)

The Arctic Domain

A Narrow Niche for Joint Special Operations Forces

By Kevin D. Stringer

Global climate change has catapulted the Arctic into the center of geopolitics, as melting Arctic ice transforms the region from one of primarily scientific interest into a maelstrom of competing commercial, national security, and environmental concerns.[1] Security in the Arctic encompasses a broad spectrum of activities, ranging from resource extraction and trade to national defense.[2] With the thawing of the ice, and Russia's expanding strategic interests in the polar region, the Arctic takes on profound importance for the international security of a number of North Atlantic Treaty Organization (NATO) and neutral Nordic states. Even if the recent reduction in Arctic ice is only a cyclical phenomenon, it still poses defense challenges in the present for these nations.[3]

While coast guard and naval forces will have primacy for this domain, special operations forces (SOF), principally maritime and air, can play a narrow but significant role in the areas of special reconnaissance (SR) and related sovereignty assertion and platform seizure missions to support polar national security objectives. SOF are ideally suited to this harsh and complex environment given their expertise, training, and resilience, which are not found in conventional military forces or law enforcement organizations. This article illustrates the growing relevance of the Arctic domain, examines Russia's expanding national interest in polar matters, and shows the potential role of SOF for several niche missions in this increasingly

Dr. Kevin D. Stringer is an Adjunct Faculty Member at the Joint Special Operations University and a Lieutenant Colonel in the U.S. Army Reserve.

relevant region. Danish and Finnish examples are highlighted to illustrate that the United States, in partnership with the other Arctic NATO and neutral nations, should focus on customizing an appropriate SOF segment to perform specified tasks, given future uncertainties in this unique ecosystem.

Climate Change, Resources, and Territorial Disputes

The Arctic covers more than one-sixth of the Earth's total land mass plus the Arctic Ocean.[4] The geopolitical significance of the Arctic Ocean increases because of growing shortages of land-based raw materials, its expected resource wealth, new conveyor and transport technologies, and progressive climatic amelioration.[5] According to the Intergovernmental Panel on Climate Change, the Arctic warms nearly twice as fast as the rest of the world. Along with rising temperatures, the Arctic has experienced a dramatic decrease in the annual extent of sea ice. This decline in sea ice coverage is particularly pronounced in September.[6] Estimates show that approximately 41 percent of the permanent Arctic ice has completely disappeared, "and every year a further million square miles or so vanishes, shrinking the ice cap to around half of the size it covered in the mid-twentieth century."[7] In fact, the U.S. Navy's "Arctic Roadmap" predicts ice-free conditions for a portion of the Arctic by the summer of 2030.[8] These spectacular changes in the Arctic environment will have a range of economic, political, and security consequences.

Arctic climate change makes the region the subject of growing international attention. The melting of the ice cap has led to speculation that new economic opportunities are opening in a region that has been frozen for centuries. Beyond commercial conjecture, the diminishment of Arctic sea ice has led to increased human activities in the Arctic and has heightened interest in, and concerns about, the region's future. The Arctic Ocean seabed is rich in mineral resources, most notably natural gas and oil. However, forecasts of greater economic activity raise concerns of competing Arctic sovereignty claims: increased commercial shipping through the Arctic; aggressive oil, gas, and mineral exploration; threats to endangered Arctic species; and expanding military operations in the region that could lead to conflict.[9]

The primary catalyst for greater Arctic activity in the wake of the receding ice cap is the potential economic value inherent in the region. For energy resources, *Science* magazine indicated that 30 percent of the world's undiscovered natural gas and 13 percent of its undiscovered oil might be found north of the Arctic Circle.[10] A 2008 U.S. Geological Survey appraisal of undiscovered oil and gas north of the Arctic Circle reinforced this view with the assertion that the "extensive Arctic continental shelves may constitute the geographically largest unexplored prospective area for petroleum remaining on Earth."[11] While more research is needed to define the resource potential accurately, the Arctic stands out as one of the most promising energy venues in the world.[12] Furthermore, the Arctic is an important commercial fishing ground, especially for the largest populations (salmon, cod, and coalfish).[13] Beyond natural resources, professional tourism, particularly polar cruises, will become more attractive as the ice melts.[14] Finally, new maritime routes from Asia to the Atlantic will create opportunities to save vast fuel costs for the shipping industry. Use of the Northwest Passage over North America could shorten transport routes between Asia and the U.S. East Coast by 5,000 miles. The Northern Sea Route over Eurasia is also important because it shortens shipping routes between northern Europe and northeast Asia by 40 percent compared with the existing routes through the Suez or Panama canals, and takes thousands of miles off sea routes around Africa or Latin America.[15]

Obviously, the Arctic emerges as an increasingly attractive market for investment and trade, based largely on the opening of new Arctic sea lines and the access they provide.[16] Considering the aforementioned commercial opportunities, Arctic politics center increasingly on access to natural resources and sailing routes, with the security interests of Arctic nations closely related to their territorial boundaries and exclusive economic zones (EEZ). Since commercial objectives are often seen as potentially conflicting rather than shared, a "zone of peace" in the sense of an Arctic security community has not yet developed.[17] This situation is exacerbated by the geography of the Arctic as a semi-enclosed sea encircled by littoral states, since extensions of continental shelves and delimitations of maritime boundaries invariably lead to overlapping sovereignty claims, which can cause interstate friction.[18] This is not a new phenomenon, though. The Canadian archipelago, for example, has been investigated, mapped, and claimed by different nations in the past.[19] Overall, the combination of melting Arctic sea ice, potential polar riches, and conflicting territorial claims creates the conditions for heightened interstate tensions among all the players. This state of affairs is further magnified by increased, yet unpredictable, Russian actions in the region.

A Russian Threat?

The Arctic is vital to Russia's relevance in world affairs. In addition to possessing the longest Arctic coastline, Russia encompasses at least half of the Arctic in terms of area, population, and probably mineral wealth.[20] As such, with its geographical location and the length of its northern coastline, Russia is a key regional player, and its future geopolitical and economic power in international matters is directly linked to its potential exploitation of valuable Arctic resources.[21] Moreover, the Arctic has always played a significant role for the Russian military, particularly its navy.[22] Consequently, Russia has a stake in essentially all contentious Arctic issues: delimitation of territory; ownership and management of economic resources, particularly natural resource deposits; and the prevention of conflict between the military forces of the Arctic coastal states, all of which are improving, to one degree or another, their Arctic-oriented defense capabilities.[23]

Russia's North is one of the country's richest areas. Its value derives from the vast quantities of precious raw materials to be found there including oil, gas, gold, diamonds, nickel, copper, platinum, iron, and timber. While the northern region of Russia is home to less than 10 percent of the population, its contribution to national revenue is about one-fifth of overall gross domestic product. Approximately 60 percent of raw materials exports come from the north of the country. Estimates show that 90 percent of Russia's gas and 60 percent of its oil can be found in the polar region. The total value of these mineral resources in Russia's North exceeds $22.4 trillion according to Western estimates. By comparison, the total value of U.S. mineral resources is $8 trillion.[24]

For Russia, the melting sea ice in the Arctic creates huge opportunities regarding accessing the oil and gas fields located within its EEZ. Of all the great powers, Russia will benefit most from Arctic changes.[25] As such, Moscow is keen to capitalize on natural resource development and shipping in the region by exploiting areas such as the Barents Sea, 540 kilometers off the coast of the Kola Peninsula and home to one of the world's biggest proven offshore gas fields.[26] Yet such exploitation will hinge on its ability to project elements of national military power into the region.

Militarily, Russia's ambitions remain lofty, and contrary to the 1990s, the political willingness and money to increase defense spending now exist. This increase in military activity in the Arctic, and Russia's assertiveness and increasingly confrontational rhetoric in foreign policy issues, are most probably only the beginning of a more visible Russian presence in the region.[27] Russia seeks to project its sovereign authority through improved border control to provide safety and security, especially in the Northern Sea Route (NSR), and to maintain credible forces to secure critical infrastructures. Russia also strives to maintain, develop, and project a convincing military force—primarily naval, aerial, and missile assets—in the region to be able to react in various politico-military scenarios as well as to deter the expansion of unwanted foreign military presence into the (Russian) Arctic.[28] The primary maritime instrument of Russian power is its Northern Fleet. While dramatically reduced from its Cold War size, the Russian Northern Fleet is the largest of the five Russian fleets and is the single most substantial combat naval force permanently deployed in the marine Arctic.[29] Apart from the Russian Northern Fleet, not a single Arctic state deploys combat naval forces in the marine Arctic, although the coast guards of these states do patrol the area. Furthermore, Arctic state ability to redeploy naval forces from other areas of operations is either limited or nonexistent since none of the other polar nations has warships designed for operation in the extreme Arctic conditions.[30]

According to Russian national security documents, Moscow plans to establish special Arctic military formations to "protect the county's national interests and to guarantee military security in different military and political situations."[31] To guard critical lines of transportation such as the NSR and to secure northern borders, then–Russian Defense Minister Anatoliy Serdyukov in July 2011 announced plans to create two special army brigades to be based in the Arctic cities of Murmansk and Arkhangelsk. This concept derived from Russian studies of specialist Arctic troops in Finland, Norway, and Sweden.[32]

This rising role of the Arctic in Russian security policy and Moscow's preparation to defend its rights to natural assets with force if needed has been accentuated by official government statements.[33] For example, in a national security document released in May 2009, the Kremlin stated that "in a competition for resources, it can't be ruled out that military force could be used for resolving problems."[34] The Russian government reinforced this view with the statement that "although it deplores the notion of an arms race in the high north and does not foresee a conflict there, it intends to protect its Arctic interests."[35] Of greater concern, however, are the security perspectives and military doctrine underlying Russia's military buildup and modernization in the Arctic. While the strategic thinking of the Russian political elite is not monolithic, a "defense-driven" zero-sum orientation dominates recent Russian strategy.[36] Such policy statements, combined with a series of Russian actions such as the resumption of strategic bomber flights over the Arctic, cyber attacks on Estonia, the Russo-Georgian War of 2008, the 2014 annexation of the Crimea, and Russian support for the insurgency in Eastern Ukraine, all contribute to growing uneasiness over future Russian intentions in the Arctic region. Among the Arctic neutral states, for instance, Sweden notes an increasing regional instability and the likelihood of crises in both the Baltic Sea and Arctic regions, which require an overall reevaluation of Swedish defense policy.[37] Similarly, rising Russian activities in the Kola Peninsula and the increasing strategic importance of the Barents Sea are forcing Finland to carefully reevaluate its defense of adjacent Lapland.[38] This overall security situation leads to a discussion of the role of SOF in this austere but potentially volatile environment.

The SOF Niche

There is debate about the future of security developments in the Arctic. Some observers postulate a remilitarization of the Arctic and the occurrence of "armed clashes" in the region sooner rather than later. Others state that both the logic of this argument and the evidence supporting it are flimsy, arguing that there is no reason to expect that matters relating to military security will rise to the top of the Arctic agenda soon.[39] While some have argued that terrorism and hijacking may constitute security concerns in the region, others maintain that such threats are chimerical, given the challenges of distance and geography and the difficulty of navigating in a polar environment.[40] Even if a direct military conflict may be unlikely, tensions with Russia may still precipitate some level of U.S. and NATO engagement in the Arctic, and SOF, with their unique capabilities and small footprint, may be the deterrent and surveillance force of choice.

In the harsh polar ecosystem, the military becomes the tool of national

Attack submarine USS *New Mexico* surfaces at Ice Camp Nautilus in Arctic Ocean during Ice Exercise 2014 (DOD/Joshua Davies)

policy almost by default. The Arctic is a complex environment, and a report by the Arctic Institute noted that "the armed forces, beyond their responsibility for handling all contingencies, are also the only agencies with both the requisite monitoring instruments and the physical capabilities to operate in such a vast and inhospitable region."[41] A further concern is that the Arctic is an environment of extreme operational challenges, even for armed forces with longstanding Arctic experience.[42] These problems range from limited communications due to magnetic and solar phenomena that reduce radio signals to environmental degradation of personnel, weapons systems, and navigation equipment. Considering the nature of SOF, with their recruitment of more experienced personnel, a rigorous selection process, high resilience, and extensive training to achieve proficiency in applicable mission sets, these elite units offer the innovative, low-cost, and small-footprint approach needed to achieve nuanced national security objectives in a challenging region.[43]

While the first decade of the 21st century has seen an enormous increase in the use of U.S. and NATO SOF for the campaigns in Iraq and Afghanistan, SOF focus has skewed to direct-action operations. These operations are defined as short-duration strikes and other small-scale offensive actions that are conducted in hostile, denied, or diplomatically sensitive environments, and which employ specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets.[44] The most visible of such activities was the elimination of Osama bin Laden in the May 2011 raid on his compound in Pakistan. This emphasis on direct action has come at a price, however, causing SOF units to neglect a number of other useful mission sets. The commander of the Colorado-based U.S. Special Operations Command North, Rear Admiral Kerry Metz, stated that over the past decade of war in the Middle East, "we've gotten out of [the habit of doing] the routine work up in the Arctic area. SOF as an entity has not focused on that area, and I think over the next few years, we're going to have to sort of return to those roots."[45] Similarly, then–Major General Brad Webb, commander of U.S. Special Operations Command Europe, affirmed, "while Africa may be the challenge for this generation the Arctic will be the challenge for the next."[46] For the Arctic, the tasks of special reconnaissance, sovereignty operations, and platform seizure missions come to the forefront for SOF employment.

Special Reconnaissance and Sovereignty Assertion

Considering Arctic climate dynamics and increased human activity on polar air, land, and sea routes, the assertion of sovereignty and the need for "on the surface" situational awareness takes on strategic significance. This requirement is compounded by key challenges that include shortfalls in ice and weather reporting and forecasting and limitations in command, control, communications, computers, intelligence, surveillance, and reconnaissance due to lack of assets and harsh environmental conditions.[47] Yet politically, sovereign presence and domain awareness are essential prerequisites for Arctic national security. For example, Norwegian Defense Minister Ine Eriksen Søreide stated that she did not want to remilitarize the [Arctic] border, but "at the same time we do have, and want to have, situational awareness for our own country and the alliance."[48] Similarly, since 2006, Canadian Prime Minister Stephen Harper has placed enormous emphasis on "exercising sovereignty over Canada's North . . . our number one Arctic foreign policy priority."[49] While these objectives can be partially attained with satellite, ship, and aerial platforms, a comprehensive knowledge of the Arctic physical environment can be achieved only by an actual human presence on the ground.

Hence, with increased activity in and over Arctic waters, a military's knowledge base will need to be improved significantly concerning the evolving operational environment in the Arctic (including newly accessible uncharted waterways), as will the military's ability to conduct search and rescue, disaster response and relief, and environmental security operations, among other essential missions, within the Arctic region. In this context, building a greater capacity for maritime domain awareness (MDA) looms as an especially critical requirement and obligation for forces assigned to the Arctic.[50] One option to achieve MDA is through the conducting of "on the surface" SR missions by SOF elements. Special reconnaissance entails reconnaissance and surveillance actions normally conducted in a clandestine or covert manner to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. SR may include collecting information on human activities or securing data on the meteorological, hydrographic, or geographic characteristics of a particular area.[51] For the Arctic, Denmark provides an excellent model for the use of SOF in SR and sovereignty operation roles, with Finland offering additional considerations for this mission.

Although the Danish armed forces currently undertake important tasks in the Arctic, including enforcement of sovereignty, Denmark's military posture there will inevitably have to adjust to take on new roles and capabilities, such as wider ranging patrol and domain awareness missions within Greenland, a desirable territory rich in both oil and precious metals.[52] The launch of the Danish Defense Force (DDF) Greenland-headquartered Joint Arctic Command in October 2012 initiated plans to expand training and deployment of special operations forces to reinforce Denmark's sovereignty over its Arctic territories, which extend to 1.6 million square miles.[53] The Arctic command organization took over responsibility for the SOF Arctic defense unit known as the Sirius Patrol, which has spearheaded the DDF's long-range reconnaissance patrols in Greenland since 1941, often operating in temperatures as low as -67°F, while overseeing sovereignty enforcement in the remote reaches of Greenland. These multiple, two-man teams with dogs operate for long periods over 160,000 square kilometers of Arctic terrain to provide real-time presence, reporting, and surveillance to assert Danish sovereignty over its polar realm. Many of the DDF's core SOF, past and present, have sharpened their survival and reconnaissance skills on Sirius missions.[54]

In addition to Denmark, Finland has significant experience in operating in hard winter conditions and is well placed to offer cold climate training and exercises to its international partners.[55] This hard-won experience is not present within many other Arctic countries, particularly in the United States. Operations in the Arctic require special cold-weather gear, tactics, techniques, procedures, and especially training for the armed forces. Finland's airmobile special forces training center in Utti (Utin Jääkärirykmentti) specializes in performing in severe Arctic conditions, with the ability to operate even when the outside temperature is as low as -40°F. This training in operating in cold climate surroundings is a tangible resource Finland could offer to other NATO or neutral Arctic nations for SOF SR and sovereignty operation missions.[56] For U.S. SOF, the SR and sovereignty missions would be best placed with selected U.S. Marine Corps Forces Special Operations Command long-range reconnaissance units, trained in Arctic conditions and using Danish and Finnish SOF expertise for extreme polar operations.

Platform Seizure Missions

Under the designation of counterterrorism tasks, hostage rescue and recovery operations are normally sensitive crisis missions in response to terrorist threats and incidents. Adapted to the Arctic—and given the low probability of terrorist activity there considering the distances involved, Arctic geography, and the overall polar environment—these missions are more likely to involve the protection of Arctic weather stations, military bases, petroleum infrastructure such as oil rigs, pipelines, terminals, and refineries, and even ships in the region from adversarial state, criminal, or environmental protester activity.[57] Such action is likely to involve the retaking of an occupied installation, offshore platform, or cruise ship, potentially with nonlethal means. In Denmark, for example, more resources will be directed at the army's and navy's main SOF units, the Hunter (*Jægerkorpset*) and Frogman (*Frømandskorpset*) corps, for this purpose. Both units, which have been extensively deployed in Afghanistan, are spending more hours on mission-specific training that requires honing the skills necessary to deal with a broad range of tasks, from assaulting enemy ships and using stealth to restoring control and sovereignty over Danish fixed oil and gas installations in the Arctic, by air or sea.[58] For the United States, Navy SEALs already have this capability in their core mission and need only to attain Arctic proficiency for this contingent polar operation. Again, leveraging Arctic-capable partner-nation SOF expertise and linking this role to the previously discussed SR task would be the most effective method for exercising this competence.

Both the SR and platform seizure tasks will require air SOF units in

U.S. Navy Arctic Submarine laboratory technician takes break from preparing submarine surfacing site near Ice Camp Nautilus in Arctic Ocean during Ice Exercise 2014 (DOD/Joshua Davies)

Two F-15C Eagles return to simulated air combat portion of Arctic Challenge exercise over Norway, helping boost interoperability among NATO, the United States, United Kingdom, and members of Nordic Defense Cooperation (U.S. Air Force/Christopher Mesnard)

support. Possible units of action for this assignment are U.S. Air Force Special Operations, MC-130P aircraft squadrons, and related CV-22 tiltrotor units, coupled with selected SOF pararescuemen and combat rescue officers from the special tactics squadrons. By locating such assets at Thule Air Base in Greenland and Joint Base Elmendorf-Richardson in Alaska, selected air SOF units could provide air coverage and support for most of the North American Arctic and Northwest Passage. Although the Air Force has assets in its conventional Service with similar profiles and equipment, air SOF may be better suited for a niche Arctic mission because of their ability to train selected crews to specialize in Arctic air and survival as well as their overall organizational linkage to SOF maritime units performing the other SR, sovereignty, and platform seizure missions in the polar environment.

While direct military conflict may be unlikely in the Arctic, the uncertainty about the direction in which developments in the region will unfold and, as a result, the uncertainty about the precise nature of the challenges and threats deriving from those developments, justify the increased attention of the international community toward the Arctic.[59] Simultaneously, Russia's bellicose actions in other regions, overall martial rhetoric, and polar military presence make its intentions unclear, and thus a key player to watch in Arctic affairs.[60] As the ice recedes and maritime passages open, the potential for territorial conflict and state-on-state confrontations could increase. Hence, this is an ideal niche situation for low-profile, small-footprint maritime and air SOF teams to monitor the region and provide presence, strategic reconnaissance, and surveillance for sovereignty purposes, as well as platform seizure or recovery capacity in readiness. For the United States, these Arctic missions require a mix of specialized maritime and air SOF that can leverage the Arctic expertise and capabilities of benchmark-setting partner nations such as Denmark and Finland, and operate in a unique joint special operations environment. JFQ

Notes

[1] Charles K. Ebinger and Evie Zambetakis, "The Geopolitics of Arctic Melt," *International Affairs* 85, no. 6 (November 2009), 1215–1232, specifically 1215.

[2] *Arctic Strategy* (Washington, DC: Department of Defense, November 2013), 2.

[3] Luke Coffey, "The Future of U.S. Bases in Europe—A View from America," *Baltic Security & Defence Review* 15, no. 2 (2013), 135.

[4] *Kingdom of Denmark Strategy for the Arctic 2011–2020* (Copenhagen: Ministry of Foreign Affairs, August 2011), 9.

[5] See Eva Ingenfeld, "Just in Case Policy in the Arctic," *Arctic* 63, no. 2 (June 2010), 257–259.

[6] Intergovernmental Panel on Climate Change (IPCC) Working Group 1 Contribution to the IPCC Fifth Assessment Report, June 7, 2013, 12–33.

[7] Roger Howard, *The Arctic Gold Rush: The New Race for Tomorrow's Natural Resources* (New York: Continuum, 2009), 8.

[8] David Titley and Courtney St. John, "Arctic Security Considerations and the U.S. Navy's Roadmap for the Arctic," *Naval War College Review* 63, no. 2 (Spring 2010), 36.

[9] Andrei Zagorski, "The Arctic: A New Geopolitical Pivot?" *Russia Direct Monthly Memo*, no. 5 (December 2013), 2; and Ronald O'Rourke, *Changes in the Arctic: Background and Issues for Congress*, R41153 (Washington, DC: Congressional Research Service, April 2014), 1.

[10] Donald L. Gautier et al., "Assessment of Undiscovered Oil and Gas in the Arctic," *Science* 324, no. 5931 (2009), 1175–1179.

[11] U.S. Geological Survey Fact Sheet 2008-3049, "Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle," available at <http://pubs.usgs.gov/fs/2008/3049/>.

[12] See Kataryna Zysk, "The Evolving Arctic Security Environment: An Assessment," in *Russia in the Arctic*, ed. Stephen Blank (Carlisle, PA: U.S. Army War College, July 2011), 91–138.

[13] Ingenfeld, 258.

[14] Vesa Virtanen, *The Arctic in World Politics. The United States, Russia, and China in the Arctic—Implications for Finland* (Boston: Weatherhead Center for International Affairs, Harvard University, 2013), available at <http://projects.iq.harvard.edu/files/fellows/files/virtanen.pdf>.

[15] Ibid.; and Ebinger and Zambetakis, 1221.

[16] Charles M. Perry and Bobby Anderson, *New Strategic Dynamics in the Arctic Region: Implications for National Security and International Collaboration* (Washington, DC: Institute for Foreign Policy Analysis, February 2012), 28.

[17] Kristian Atland, "Russia and Its Neighbors: Military Power, Security Politics, and Interstate Relations in the Post-Cold War Arctic,"*Arctic Review on Law and Politics* 1 (February 2010), 295.

[18] Ebinger and Zambetakis, 1227; and Claudia Cinelli, "The Law of the Sea and the Arctic Ocean," *Arctic Review on Law and Politics* 2, no. 1 (2011), 4–24.

[19] Ingenfeld, 258.

[20] Zysk, "Evolving Arctic," 97; "The Arctic: Special Report," *The Economist*, June 16, 2012, 11; and Barbora Padrtova, "Russian Approach Towards the Arctic Region," in *Panorama of Global Security Environment 2012*, ed. M. Majer, R. Ondrejcsak, and V. Tarasovic (Bratislava: Centre for European and North Atlantic Affairs, 2012), 339–350.

[21] Virtanen.

[22] Padrtova.

[23] Perry and Anderson, 50.

[24] Valery P. Pilyavsky, "Russian Geopolitical and Economic Interest," *Friedrich Ebert Stiftung Briefing Paper*, March 2011; and Padrtova, 341.

[25] Virtanen.

[26] Atland, 280; and O'Rourke, 54.

[27] See Katatzyna Bozena Zysk, *Russian Military Power and the Arctic* (Brussels: EU-Russia Centre, October 2008); and Virtanen.

[28] Mikkola Kaplya and Harri Juha, "The Global Arctic: The Growing Arctic Interests of Russia, China, the United States and the European Union," The Finnish Institute of International Affairs Briefing Paper 133, August 2013, 4; and Padrtova, 347.

[29] Zagorski, 6; and Virtanen.

[30] Zagorski, 6.

[31] *Strategia natsional'noi bezopasnosti Rossiiskoi Federatsii do 2020 goda*, 2009, Sovet Bezopasnosti Rossiiskoi Federatsii, available at <www.scrf.gov.ru/documents/1/99.html>; and *Osnovy gosudarstvennoi politiki Rossiiskoi Federatsii v Arktike na period do 2020 goda i dalneishuiu perspektivu*, September 2008, Sovet Bezopasnosti Rossiiskoi Federatsii, available at <www.scrf.gov.ru/documents/15/98.html>.

[32] "Russia Plans Arctic Army Brigades," BBC News, July 1, 2011, available at <www.bbc.co.uk/news/world-europe-13997324>; and Padrtova, 345.

[33] Virtanen.

[34] Roger Howard, "Russia's New Front Line," *Survival* 52, no. 2 (April–May 2010), 141–155.

[35] O'Rourke, 62; and Virtanen, 45.

[36] Perry and Anderson, 64.

[37] Justyna Gotkowski, "Swedish Security in Crisis," Centre for Eastern Studies, February 13, 2013.

[38] Virtanen, 45, 5.

[39] Oran Young, "Arctic Politics in an Era of Global Change," *Brown Journal of World Affairs* 19, no. 1 (Fall/Winter 2012), 165–178, specifically 169.

[40] "The Arctic: Special Report," *The Economist*, June 16, 2012, 10.

[41] O'Rourke, 59; and Ebinger and Zambetakis, 1218.

[42] Zysk, "Evolving Arctic," 109.

[43] *Arctic Strategy*, 7.

[44] Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: Joint Chiefs of Staff, April 18, 2011), II-5–II-6.

[45] Paul McLeary, "U.S. Special Ops Commanders: We Need ISR in Africa, Comms in Arctic," *Defense News*, May 20, 2014, available at <www.defensenews.com/article/20140520/DEFREG02/305200052/US-Special-Ops-Commanders-We-Need-ISR-Africa-Comms-Arctic>.

[46] Ibid.

[47] O'Rourke, 66.

[48] Julian E. Barnes, "Cold War Echoes Under the Arctic Ice," *Wall Street Journal*, March 24, 2014, available at <http://online.wsj.com/news/articles/SB10001424052702304679404579461630946609454>; and O'Rourke, 64.

[49] Government of Canada, "Statement on Canada's Arctic Foreign Policy: Exercising Sovereignty and Promoting Canada's Northern Strategy Abroad," August 2010, available at <www.international.gc.ca/polar-polaire/assets/pdfs/ CAFP_booklet-PECA_livret-eng.pdf>.

[50] Perry and Anderson, 172.

[51] JP 3-05.

[52] *Kingdom of Denmark Strategy for the Arctic 2011–2020*, 13; and Perry and Anderson, 71.

[53] Gerard O'Dwyer, "Denmark Boosts Resources for the Arctic," *Defense News*, October 8, 2013.

[54] Ibid.; *Kingdom of Denmark Strategy for the Arctic 2011–2020*, 21; Mia Bennett, "Denmark's Strategy for the Arctic," Foreign Policy Association, November 14, 2011, available at <http://foreignpolicyblogs.com/2011/11/14/denmarks-strategy-for-the-arctic/>; and "Greenland by Dog Sledge: The Sirius Patrol in Numbers," BBC News, November 30, 2011, available at <www.bbc.co.uk/news/magazine-15940985>.

[55] *Finland's Strategy for the Arctic Region 2013* (Helsinki: Prime Minister's Office, August 2013), 14.

[56] Virtanen, 93.

[57] JP 3-05, xi; and Atland, 279–298, specifically 284.

[58] O'Dwyer.

[59] Zysk, "Evolving Arctic," 117.

[60] Atland, 280.

U.S. Central Command–directed, irregular warfare–themed exercise Eager Lion with U.S. Marines and Jordanian military focuses on missions U.S. forces and coalition partners might perform during global contingency operations (DOD/Richard Blumenstein)

Rapid Regeneration of Irregular Warfare Capacity

By Stephen Watts, J. Michael Polich, and Derek Eaton

There is widespread agreement among the public and in the foreign and defense communities that the United States should avoid "another Iraq" or "another Afghanistan"—that is, another large-scale, long-term, and high-cost stability operation. President Barack Obama's reluctance to put "boots on the ground" in Iraq is but the most recent example of this reaction against the high costs and questionable outcomes of the conflicts in those two countries. Former Defense Secretary Robert Gates may have been particularly blunt when he declared that anyone advising a future President to pursue forcible regime change in the developing world "should have his head examined," but the sentiment is widespread.[1]

Worse than having to fight another Iraq or another Afghanistan, however, would be if the United States were yet again unprepared for such a contingency—as occurred when it divested itself of counterinsurgency capabilities after the policy community united against

Stephen Watts is a Political Scientist at the RAND Corporation. J. Michael Polich is a Senior Behavioral Scientist at the RAND Corporation. Derek Eaton is an Associate Political Scientist at the RAND Corporation.

"another Vietnam." This article considers the challenge of maintaining readiness for large-scale irregular warfare (IW) contingencies when the national mood has so decisively turned against such operations.

The need to hedge against such a contingency is recognized in both the 2012 Defense Strategic Guidance and the 2014 Quadrennial Defense Review (QDR). Whereas both documents are widely interpreted as rejecting large-scale counterinsurgency and stability operations, they actually provide more nuanced guidance. Although U.S. forces will not be *sized* to conduct such operations, the QDR insists that "we will preserve the expertise gained during the past ten years of counterinsurgency and stability operations [and] protect the ability to regenerate capabilities that might be needed to meet future demands."[2] It is less clear what this guidance means in practice. To sketch the outlines of such an "adaptability hedge,"[3] we first review the history of large-scale IW operations to determine the timelines that intervening forces have historically needed to adapt to such contingencies, how quickly they have adapted in practice, and the costs of slow adaptation. Second, we examine the sorts of ground forces that are typically required for such operations and—using simple metrics—estimate the amount of time required to regenerate them. Based on this analysis, we suggest which capabilities could be regenerated relatively quickly for large-scale IW contingencies as the need arises and which would be priorities to keep in the ground force structure due to the long lag times associated with rebuilding these capabilities once they are lost. Finally, we briefly review the pipeline for regenerating IW capabilities and how to ensure the pipeline could function rapidly if needed.

The Imperative of Rapid Adaptation for Large-Scale IW

Even if they accept that the United States might at some point get drawn into another such contingency, many observers are skeptical of making sizable investments in standing capabilities for large-scale IW. These skeptics generally make three arguments. First, because insurgencies typically last many years, intervening forces have considerable time to adapt to the operational theme and environment.[4] In contrast, conventional contingencies may conclude in victory or defeat in mere weeks. If one cannot pay the price necessary to be prepared for every kind of conflict, it is better to be prepared for conventional contingencies and, if necessary, adapt over time to irregular warfare rather than vice versa. Second, IW is typically fought by small units on a highly decentralized battlefield—a much easier task *militarily* than coordinating fire and maneuver across large numbers of higher echelon formations. The skeptics of IW investments maintain it is easier to adapt from more complex military tasks to less complex ones than it is to go in the other direction.[5] Again, such an argument suggests that the bulk of investments should be made in conventional warfighting capabilities. Finally, skeptics of IW contend that counterinsurgency and stability operations have historically been "wars of choice" fought by the United States in less strategically vital regions of the world. These skeptics maintain that if fiscal austerity imposes the need for U.S. Armed Forces to accept a higher degree of risk than usual, this risk is best assumed in less-vital IW capabilities.

While defensible, each of these arguments overstates its case and minimizes the extent of the risk the United States would incur by failing to invest in standing IW capabilities or the ability to regenerate them quickly.

How Long Do Militaries Have to Adapt to IW? The answer to this question in any particular case obviously depends on circumstances. But history provides an approximate answer that can be used for force planning. While insurgencies typically last for more than 10 years (15 years, more recently), *foreign* militaries usually intervene in them for much shorter periods of time—at least when they are deployed in large numbers by democracies. Looking at the best-known cases of expeditionary counterinsurgency by democratic interveners, we see that democracies that have deployed 25,000 or more forces have done so for only 5 years on average, and rarely—if ever—for more than 8 years.

Even these numbers, however, probably overstate the amount of time a democratic power such as the United States has to adapt to the requirements of IW. For instance, although the United States deployed large numbers of forces in South Vietnam from 1965 to 1972, it was searching for a way out after the Tet Offensive in January–February 1968—a mere 3 years after escalating its involvement. Similarly, the United States intervened on a large scale in Iraq from 2003 to 2011, but by 2007—less than 4 years after its invasion—the United States had committed to either win the war through the so-called surge or withdraw. And the United States is not alone in this respect. In the case of the large-scale French counterinsurgency in Algeria (1954–1962), many observers argue the war became unwinnable for France as a result of its widespread use of torture in the Battle of Algiers, which ended in 1957—3 years after the escalation of French involvement. Similarly, India completely withdrew its forces from large-scale counterinsurgency operations in Sri Lanka within 3 years (1987–1990), and Israel withdrew the bulk of its forces from Lebanon in less than 2 years (1982–1983).

In short, there appears to be a small window of time before an intervening democracy such as the United States reaches a "culminating point" by which it must be on a clear path to an acceptable outcome or face strong domestic political pressures to withdraw.

How Long Does It Take to Adapt to the Requirements of IW? There is no way to measure exactly what "good enough" adaptation looks like and how long it has taken across a range of contingencies. Instead, an examination of a single case—the U.S. experience in Operation *Iraqi Freedom* (OIF)—is helpful to illustrate how long it took U.S. forces to adapt in a recent war.

There is some debate about what constituted sufficient adaptation in Iraq and how long it took. A few observers—mostly counterinsurgency skeptics—argue that U.S. forces adapted within the first year of their deployment in theater.[6] Others, however, point to General Stanley McChrystal's memorandum of November 2009 outlining counterinsurgency guidance for forces in Afghanistan as evidence that substantial portions of the force still had not mastered critical aspects of IW.

But a review of the literature suggests that these observers are outliers. Most sources agree that U.S. forces required 3½ to 4 years to adapt at least reasonably well to the exigencies of OIF. There is widespread acknowledgment that the U.S. military was initially ill-prepared for the insurgency it encountered in Iraq despite the efforts of individuals to do the best they could with what they had under extraordinarily trying circumstances. A survey by Colonel William Hix and Kalev Sepp reportedly found that only one-fifth of units demonstrated counterinsurgency proficiency in August 2005.[7] On the basis of detailed examination of multiple units, one of the best empirical studies of adaptation in OIF found that many of the key breakthroughs occurred in 2006 and early 2007.[8] A Joint Staff–sponsored retrospective on Iraq and Afghanistan concluded that:

> *operations during the first half of the decade* [through 2006] *were often marked by numerous missteps and challenges as the U.S. government and military applied a strategy and force suited for a different threat and environment. Operations in the second half of the decade often featured successful adaptation to overcome these challenges.*[9]

Three problems of adaptation in the early years of OIF stand out from these various studies: insufficiently discriminate use of force, inadequate nonlethal enablers to conduct effective civil-military and intelligence operations, and insufficient (and often inappropriate) resources devoted to the advisory (foreign internal defense) function. These problems are summarized in table 1.

Table. Commonly Identified Adaptation Failures in the Early Years of Operation *Iraqi Freedom*

Lethal Operations	Civil-Military Operations and Nonlethal Enablers	Foreign Internal Defense (FID)
Over-emphasis on offensive operations, inadequately discriminate use of firepower Concentration of forces rather than dispersion in COPs Lack of cultural awareness and sensitivity Failure to propagate new, full-spectrum doctrine Failure to ensure appropriate kinetic training	Failure of strategic planning Failure to ensure full-spectrum training Leaders inexperienced with coordinating multiple LOOs across civil, military spheres Inadequate numbers of trained, experienced personnel for civil functions, including reconstruction, IO Intelligence capabilities inadequate in personnel levels, training, and organization	Failure to prioritize FID for first year, then failure to develop realistic expectations Failure to plan for FID mission Failure to widely embed advisors with host nation forces Inadequate numbers of personnel Poor training for advisors Inappropriate personnel chosen as advisors (inappropriate background/experience and/or poor quality)

The math is both clear and troubling. On average, countries such as the United States have only 5 years (at best) to adapt to the requirements of large-scale irregular warfare abroad before they come under extraordinary political pressure to draw down their presence. But the United States recently required between 3½ and 4 years to adapt at least reasonably well to these sorts of contingencies.[10] In other words, the United States was ill-adapted to the requirements of IW for—at a minimum—approximately two-thirds to four-fifths of the time that it has typically had to fight such wars on a large scale.

What Are the Consequences of Being Poorly Adapted to the Requirements of IW? Slow adaptation entails one of two costs: either worse outcomes, or higher costs paid to obtain the same outcome. The former has been framed in terms of a so-called golden hour, the early period in an intervention during which popular expectations are set and insurgents can begin to organize. Once formed, popular expectations can become highly resistant to change, making it extremely difficult for counterinsurgents to gain popular backing after a poor start. Moreover, insurgents are at their most vulnerable when they first start to organize, making it critical that counterinsurgents are effective in this early stage. Once violence and instability spread, they provide opportunities for additional latent conflicts to turn violent and for hatreds and suspicions to harden, leading to an intensification of the conflict. Observers have detected such dynamics in the U.S. "attritional" strategy in Vietnam as well as in Iraq and Afghanistan. While counterinsurgents can still potentially obtain their objectives in the end even if they perform poorly in the early days of a conflict, the price is likely to be much steeper.[11]

Nor is IW likely to be confined to peripheral regions of little strategic significance to the United States as contended by skeptics of significant investments in maintaining the ability to quickly regenerate large-scale IW capabilities. Many observers of conflict trends believe that irregular and conventional warfare are likely to blend in so-called hybrid conflicts.[12] In looking to potential future conflicts, most of the ones that appear to be both relatively more likely to occur and most significant in their impact involve likely hybrid threats—contingencies such as state collapse and loose nuclear materials in North Korea or a future nuclear-armed Iran. IW does not represent a set of lesser strategic concerns for the United States—"wars of choice" that can be easily avoided. To the contrary, IW is a likely element of many or most of the highest-risk scenarios the United States currently faces.

Rapid Adaptation to Large-Scale IW

Building readiness for future IW contingencies is not fundamentally different from building readiness for other types

Survival evasion resistance and escape specialist and rescue squadron flight engineer Airmen conduct combat survival training near Osan Air Base, South Korea, during 2012 Pacific Thunder exercise (DOD/Sara Csurilla)

of war. As in all readiness debates, policymakers face tradeoffs among cost, military effectiveness, and time.[13] In this era of fiscal constraints, policymakers are seeking to limit costs by reducing military readiness for large-scale IW contingencies, while still paying for the necessary infrastructure to regenerate such capabilities quickly if needed.

This approach is reasonable in principle. In practice, it requires answering difficult questions: How quickly can such capabilities be regenerated? Can they be regenerated quickly enough, given the relatively short timelines for IW adaptation discussed in the previous section? Capabilities in high demand for IW that can only be built or achieve adequate readiness over long periods of time are candidates to be retained as forces in being. Capabilities required for IW that can be built or achieve readiness relatively quickly are candidates to be regenerated on demand. Once we know which capabilities need to be kept as forces in being, and what infrastructure is necessary to maintain a pipeline to regenerate other forms of IW capacity, we can determine (at least roughly) the price tag associated with the 2014 QDR's pledge to "preserve the expertise gained during the past ten years of counterinsurgency and stability operations [and] protect the ability to regenerate capabilities that might be needed to meet future demands."

Estimating Requirements for Capabilities in Being. Once the need for adaptation is recognized, it can occur in many domains relatively quickly. Training and doctrine, for instance, can be oriented toward the specific circumstances of new irregular contingencies within as little as a few months. Similarly, facilities can be adapted, with mockups of foreign villages built and role-players hired on a contract basis, in relatively short order. Such adaptations are necessary, and the following section will detail some of the infrastructure necessary to ensure they are executed rapidly. But for IW, the long pole in the tent is typically human capital—the development of military leaders who can rely on the education and experience they have gained over many years (or even decades) to adapt to a complex environment. Such leaders cannot be regenerated quickly if decisionmakers have guessed incorrectly about the nature of future contingencies.[14]

What types of leaders are most in demand? Studies have found that several types of units were particularly stressed by IW requirements in Iraq and Afghanistan: combat arms, rotary aviation, military intelligence (especially

Airmen of 22nd special tactics squadron jump from MC-130H Combat Talon II during Emerald Warrior, DOD's only irregular warfare exercise (U.S. Air Force/ Marleah Miller)

assets related to human intelligence), military police (particularly law enforcement), explosive ordnance disposal (EOD), and special operations forces (SOF).[15] Nor are these demands unique to Iraq and Afghanistan; many of these same types of units were in high demand in a variety of other IW campaigns, both counterinsurgency (in Vietnam) and other forms of stability operations (for instance, in Bosnia and Kosovo).

Unfortunately, many of the types of units in highest demand for IW are rank-heavy formations filled with personnel with many years of experience in their fields. For example, personnel comprising a Brigade Combat Team (BCT) possess approximately 4 years of service on average. Many enablers, such as transportation or administrative units, require far less experience; the personnel in quartermaster companies or light- and medium-truck companies possess approximately 3 years of service on average. In contrast, many of the enablers in high demand for IW contingencies possess personnel with considerably more experience. Personnel in interrogation battalions, law and order detachments, tactical military information support operations detachments, civil affairs teams, and EOD companies all possess between 5 and 7 years of service on average—approximately twice that of the logistical support units discussed above and substantially higher than the experience in a BCT. Moreover, the average years of service in these units is approximately as long as the United States ever remains committed on a large scale to IW contingencies. Regenerating these capabilities on demand, in other words, is probably not practical unless decisionmakers are willing to accept dramatic declines in quality, no matter how large the pipeline for regeneration.

Capabilities that are in high demand for IW and have lengthy development times are high-priority candidates to be retained in disproportionately large numbers if the Department of Defense (DOD) makes a commitment to quickly regain critical IW proficiencies and capacity. These capabilities include aviation, certain types of military intelligence, law enforcement, EOD, and SOF. They could be retained as formed units, or their leadership could be retained in disproportionately large numbers in a "grade over-structure" or cadre that would serve as the basis for regenerating fully formed units in times of need.[16] Regardless of how these capabilities are maintained, DOD needs to ensure that it gains appropriate experience operating in real-world environments, ideally through security cooperation and similar activities. True proficiency in tasks conducted in "wars among the people" is simply too difficult to attain in the classroom or in artificial training environments.

Maintaining a Pipeline to Regenerate Other IW Capabilities. Clearly, the United States cannot afford to maintain all the capabilities it needs for large-scale IW in capacities sufficient to meet the requirements of many plausible scenarios. Particularly where regeneration times are relatively rapid (for capabilities that require relatively less expertise) or where the overall numbers of forces involved make it impractical to maintain a force optimized for IW (as is the case for combat arms other than SOF), the United States will need to regenerate capacity and proficiency for IW as quickly as possible.

Three elements of the Services' activities are especially important in providing a basis for regenerating IW capability in the future: organizations, exercises, and school curricula. To ensure that the Services maintain their pipelines for regenerating IW capabilities, DOD should ensure adequate funding and attention for each of these elements.

Both the Army and Marine Corps created many organizations to develop proficiency for large-scale IW during the wars in Iraq and Afghanistan. The Army's focal point for this area was the Army Irregular Warfare Fusion Cell, which helped to coordinate IW-related activities among the U.S. Army Peacekeeping and Stability Operations Institute, Asymmetric Warfare Group, Center for Army Lessons Learned, and U.S. Army Special Operations Command. Similarly, the Marine Corps established the Center for Irregular Warfare, Security Cooperation Group, and Center for Advanced Operational Culture Learning. These organizations that study and codify IW operations formed DOD's intellectual foundation for preserving expertise.

In a period of fiscal constraint, these organizations' budgets have already come under pressure; the Army Irregular Warfare Fusion Cell, for instance, closed on October 1, 2014.[17] There is ample precedent to anticipate further such cuts. Service culture celebrates command functions and operational experience, and the leadership is largely drawn from the warfighting branches. If money and manpower allocations are tight, Service priorities are likely to favor deployable units and operational functions over institutions—like IW organizations—whose product is less tangible and longer term. For example, the post–Cold War drawdown resulted in sizable reductions in Army institutions (particularly at the U.S. Army Training and Doctrine Command). Similarly, when units were under pressure to deploy at full strength during the 1990s, the Army moved to increase manning in operational units at the expense of manning in the its institutional base. Therefore, we should expect that lower priorities are likely to be accorded to doctrine writers, training developers, experts in training/advising foreign forces, and even experts at the combat training centers. For these reasons, DOD should monitor the size of IW institutions and the seniority of their staff to assess their well-being and capacity to contribute to preserving IW capabilities.

Just as the Services developed organizations to gain IW proficiency over the past decade, they also oriented their training programs to the requirements of the wars in Iraq and Afghanistan. With the withdrawal of most American troops from both countries and the rebalancing of U.S. defense capabilities toward the Asia-Pacific region, the Services are justifiably reorienting their training to regain proficiency in conventional warfighting. Yet this reorientation does not mean the Services have abandoned IW. In fact, both the Army and Marine Corps have adopted scenarios based on hybrid threats, and both plan to incorporate these features into their major exercises. Steps have already been taken to test and refine these concepts.

As with institutional budgets, however, training budgets are also coming under pressure. Moreover, there are a finite number of days in a year, making it difficult to retain proficiency in as many operational themes as might be desirable. Consequently, DOD should also monitor IW proficiency by monitoring units' performance at the Services' premier exercises, such as the Army's combat training centers and Marine Corps' predeployment exercises. DOD should track data on the content of exercises (goals, types of threats, operational environment, tactics executed and evaluated, and so forth), performance of the trainee units,[18] and percentage of leaders in key positions—battalion commanders, S-3s, executive officers, company commanders—who actually execute a premier exercise rotation emphasizing IW skills during their tenure in that position.

Assuming that the scale of current operations declines as expected, fewer military leaders will have direct experience in IW. As a result, professional education courses will represent a critical means through which IW knowledge and skills will be inculcated in future cohorts of officers and noncommissioned officers. School curricula, however, are limited in the amount of student instructional time available; each domain of expertise must compete with others for curriculum hours (or "blocks of instruction"). How, then, could defense leadership monitor the curriculum profile to gauge the adequacy of IW focus? Previous studies have made a start by calculating occurrence of key words and phrases related to IW.[19] A more complete monitoring effort would establish goals and criteria for determining which skills and knowledge are most important and then use small panels of knowledgeable veterans (preferably at the O-4 or O-5 level, who have IW experience and some academic research training) to monitor and track the extent to which these skills are taught in professional military education at all levels.

DOD cannot afford to maintain the Services' current levels of proficiency in IW, nor is it necessary to do so for the majority of U.S. forces. Outside of the high-demand, long-development time capabilities for IW discussed above—capabilities such as aviation, law enforcement, certain types of military intelligence, EOD, and SOF—the goal should be rapid regeneration of IW readiness should such a contingency require it. Maintaining organizations dedicated to retaining U.S. intellectual foundations for such warfare, continuing to require some degree of proficiency in IW in the Services' key exercises, and continuing to give substantial attention to IW topics in school curricula should all help to speed the regeneration process.

Conclusion

As much as all Americans may wish to avoid another Iraq or another Afghanistan, the country cannot afford to allow its capabilities for large-scale irregular warfare to atrophy as it did when decisionmakers insisted the United States would never again fight another Vietnam. Although the United States should certainly avoid such conflicts whenever possible, trends in violent conflict toward hybrid wars suggest that it would be prudent to invest in a hedge against the possibility of U.S. involvement in another such war.

Determining the precise composition of such a hedge or its pricetag is beyond the scope of this article. Instead, we have emphasized four critical points about the broad outlines of such an IW hedge.

First, adaptation to irregular warfare is a lengthy process and the United States is unlikely to have much time to adapt to such conflicts before it comes under considerable political pressure to demonstrate tangible progress or draw down its forces.

Second, the costs of being poorly adapted to IW are substantial. Poor adaptation significantly reduces the likelihood of achieving acceptable outcomes and raises the price of whatever success is realized. Moreover, we cannot be confident that poor readiness for IW represents "acceptable risk" because IW contingencies are likely to occur only where peripheral U.S. interests are engaged. To the contrary, many highly plausible and high-impact scenarios entail substantial IW elements.

Third, the ability to adapt rapidly to large-scale IW requires both maintaining certain capabilities in being and maintaining the pipeline to regenerate other capabilities. Those capabilities that are both in high demand for IW contingencies and that depend on senior leaders—particularly certain capabilities in aviation, military intelligence, law enforcement, EOD, and SOF—represent priority candidates for retention in larger numbers as forces in being, either as formed units or in a grade over-structure or leadership cadre.

Finally, DOD should closely monitor resources and readiness levels associated with the pipeline to regenerate IW proficiency between maneuver and other forces as needed.

It should be Americans' fervent hope that such investments in rapid adaptation for large-scale irregular warfare prove unnecessary. But hope, as they say, is not a policy. As the 2014 QDR recognizes, hedging against such contingencies represents sound policy. Now it is time to ensure the resources follow to make good on such policy commitments. JFQ

Notes

[1] Thom Shanker, "Warning Against Wars Like Iraq and Afghanistan," *New York Times*, February 25, 2011.

[2] *Quadrennial Defense Review 2014* (Washington, DC: Department of Defense [DOD], March 2014), vii.

[3] This article is adapted from a classified study conducted by the RAND Corporation for the Office of the Under Secretary of Defense for Personnel and Readiness. See Stephen Watts et al., *Adaptable Ground Force Structure for Irregular Warfare*, RR-120-OSD (Santa Monica, CA: RAND Corporation, 2014).

[4] On the contention that there is adequate time to adapt to the requirements of irregular warfare (IW), see, for instance, Gian P. Gentile, "A Strategy of Tactics: Population-centric COIN and the Army," *Parameters*, Autumn 2009, 5–6.

[5] When asked which of the possible future challenges the Army should prepare for, the incoming head of the U.S. Army War College, Major General Tony Cucolo, stated, "You focus on the hardest one. . . . The hardest one is high-intensity combat operations. . . . [I]f we focus on 'deter and defeat,' I firmly believe we can do almost anything else." Quoted in Sydney J. Freedberg, Jr., "Wake Up and Adapt, Incoming War College Chief Tells Army," *AOL Defense*, April 3, 2012, available at <http://defense.aol.com/2012/04/03/wake-up-and-adapt-incoming-war-college-chief-tells-army/?icid=related1)>.

[6] See Gian P. Gentile, "Misreading the Surge Threatens U.S. Army's Conventional Capabilities," *World Politics Review*, March 4, 2008.

[7] Cited in James A. Russell, *Innovation, Transformation, and War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005–2007* (Stanford, CA: Stanford University Press, 2011), 5.

[8] Ibid. See also Thomas R. Mockaitis, *The Iraq War: Learning from the Past, Adapting to the Present, and Planning for the Future* (Carlisle, PA: U.S. Army War College, 2007); and Chad C. Serena, *A Revolution in Military Adaptation: The U.S. Army in the Iraq War* (Washington, DC: Georgetown University Press, 2011).

[9] Joint and Coalition Operational Analysis (JCOA), *Decade of War, Volume I: Enduring Lessons from the Past Decade of Operations* (Washington, DC: JCOA, June 15, 2012).

[10] The United States is not alone in this regard. On other nations' experience with slow adaptation, see Rod Thornton, "Getting It Wrong: The Crucial Mistakes Made in the Early Stages of the British Army's Deployment to Northern Ireland (August 1969 to March 1972)," *Journal of Strategic Studies* 30, no. 1 (2007), 73–107; and John Kiszely, "Learning About Counterinsurgency," *RUSI Journal*, December 2006, 16–21.

[11] Perhaps the single most commonly cited source on poor adaptation to irregular warfare is Andrew Krepinevich's study of the U.S. Army's slow adaptation to the realities of the Vietnam War and its implications for outcomes; see Andrew F. Krepinevich, Jr., *The Army and Vietnam* (Baltimore: The Johns Hopkins University Press, 1986). For a more recent similar treatment of the slow adaptation of American warfighting approaches to the context of Vietnam, see Lewis Sorley, *A Better War: The Unexamined Victories and Final Tragedy of America's Last Years in Vietnam* (San Diego: Harcourt, Inc., 1999). For an examination of the costs of slow adaptation in Afghanistan, see Daniel Marston, "Realizing the Extent of Our Errors and Forging the Road Ahead," in *Counterinsurgency in Modern Warfare*, ed. Daniel Marston and Carter Malkasian (Long Island City, NY: Osprey Publishing, 2008). On "golden hours" generally and the costs of slow adaptation in Iraq specifically, see James Stephenson, *Losing the Golden Hour: An Insider's View of Iraq's Reconstruction* (Washington, DC: Potomac Books, Inc., 2007). On the broader military implications of the golden hour, see Andrew F. Krepinevich, Jr., *An Army at the Crossroads* (Washington, DC: Center for Strategic and Budgetary Assessments, 2008), 47–54. On insurgent organization and vulnerability, see Steven Metz, *Learning from Iraq: Counterinsurgency in American Strategy* (Carlisle, PA: U.S. Army War College, 2007); and Mark Irving Lichbach, *The Rebel's Dilemma* (Ann Arbor: University of Michigan Press, 1995).

[12] Proponents of this view include former Defense Secretary Robert M. Gates, "A Bal-

Jordanian F-16 Fighting Falcon leads another Jordanian F-16, American F-16, and two Marine F-18s over training base in Northern Jordan as part of Eager Lion exercise (U.S. Air National Guard/John P. Rohrer)

anced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs* 88, no. 1 (January/February 2009), 3; Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (1st Quarter 2009), 34–48; and T.X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2006). This view has since become embedded in a wide range of Defense Department doctrinal publications.

[13] Richard K. Betts, *Military Readiness: Concepts, Choices, Consequences* (Washington, DC: Brookings Institution Press, 1995).

[14] The *2012 Army Strategic Planning Guidance* states, "The development of mid-grade officers and non-commissioned officers has been the historical limiting factor in expansibility. Experienced and effective leaders are not grown quickly." See *2012 Army Strategic Planning Guidance* (Washington, DC: Headquarters Department of the Army, April 19, 2012), 12.

[15] See Michael L. Hansen et al., *Reshaping the Army's Active and Reserve Components*, MG-961-OSD (Santa Monica, CA: RAND Corporation, 2011), 32–35; and Donald P. Wright and Timothy R. Reese, *On Point II: Transition to the New Campaign* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008).

[16] See Watts et al. for more precise analysis of historical IW utilization and the characteristics of the priority capabilities for retention.

[17] Kevin Lilley, "Irregular Warfare Center to Close Oct. 1," *Army Times*, September 1, 2014.

[18] For a related evaluation effort, see Bryan W. Hallmark and James C. Crowley, *Company Performance at the National Training Center: Battle Planning and Execution*, MR-846-A (Santa Monica, CA: RAND Corporation, 1997).

[19] Stephen J. Mariano, "Between the Pen and the Sword: 40 Years of Individual and Institutional Attitudes Toward Small Wars," Harvard University, Weatherhead Center for International Affairs, 2012 (PowerPoint briefing summarizing a Ph.D. thesis in war studies at the Royal Military College of Canada).

U.S. Naval War College student participates in National Security Decision Making seminar (U.S. Navy/James E. Foehl)

Quo Vadis? The Education of Senior Military Officers

By Charles D. Allen

This article considers approaches to teaching senior military officers at the U.S. Army War College (USAWC). It reviews the results of several studies and surveys from the employers of our graduates and from recent graduates themselves on how best to prepare for future assignments. It examines the tensions between theoretical and utilitarian education in strategy and concludes with a recommendation that USAWC faculty design and implement a portfolio approach to provide students with the opportunity to demonstrate the benefits of senior-level education.

Colonel Charles D. Allen, USA (Ret.), is Professor of Leadership and Cultural Studies in the Department of Command, Leadership, and Management at the U.S. Army War College.

Introduction

Over the past decade, the U.S. military has encountered challenges and difficulties in providing governmental services to indigenous populations. Lessons from post–World War II Europe and Japan should have informed recent U.S. policy and operations in Iraq and Afghanistan. Donald Kettl and James Fesler describe public administrators as unelected public servants who work in public departments and agencies, including the Department of Defense (DOD), at all levels of government.[1] Arguably, the U.S. military plays a substantial role in the public administration of the will of the American people. Accordingly, its educational programs should prepare them for this role. DOD consumes over 50 percent of the Nation's discretionary budget as it employs a uniformed and civilian workforce of over 3 million people. Its military officers have significant responsibilities as public administrators. Given the vast responsibilities of this largest executive branch organization, it is curious that military education programs have been generally ignored in public administration literature.[2] Like other U.S. public administrators, DOD officers both at home and abroad assume responsibilities in public security and law enforcement, in public works, and in emergency management and services. Thus, DOD senior-level education should prepare its graduates, among other things, to serve as effective public administrators.

The U.S. Army War College is one of DOD's senior-level colleges and provides the capstone of joint professional military education for U.S. military officers. Mostly in their mid-40s and with more than 20 years of service, these military professionals are high performers with extensive experience in leading and managing organizations. This formal professional development opportunity provides them a foundation for future high-level service. Each year approximately 300 officers from across the Armed Forces participate in USAWC seminars of the Resident Education Program (REP) throughout a 10-month opportunity to "confer on the three great problems of national defense, military science, and responsible command."[3] The Distance Education Program engages over 700 students in two 2-year cohorts. Like the other senior Service colleges, USAWC programs are designed to equip graduates with critical thinking skills that facilitate analysis of strategic situations, enable them to provide sound assessments and advice to senior leaders, and prepare them to manage complex national security organizations in the joint, interagency, international, and multinational environment.

The USAWC REP curriculum is delivered by three academic departments: National Security and Strategy; Command, Leadership, and Management; and Military Strategy, Plans, and Operations. The curriculum currently consists of five core courses followed by two terms of electives, along with special programs providing in-depth study of selected areas. Seminar cohorts of 16 to 17 students are led by a three- to four-person faculty team. As of academic year 2012–2013, there are 24 seminars with standardized lesson plans designed by the faculty (up from 20 seminars in 2011). Each faculty team has leeway in the delivery of content and is responsible for achieving lesson objectives for each session.

As an educational institution, USAWC should be the role model of a learning organization[4] within DOD. Organizational scholar Peter Senge asserts in *The Fifth Discipline* that a learning organization is "continually expanding its capacity to create its future."[5] The future we seek to create is one of relevancy to the military members of our society who are charged with protecting U.S. national values and interests. Thus, we continually assess the design and delivery of the curriculum to provide graduates with the best possible preparation for future service. The faculty conducts an examination of each core course and individual lessons therein—a crucial and often painful experience. My experiences in these "hot washes" or "after action reviews" generated this article on the education of USAWC students.

The Stimulus

At an end-of-course review with teaching colleagues for the REP, I was the leader of a small group for a subset of lessons of our core course on Strategic Leadership. What followed was a pointed discussion on the faculty role in educating our students for senior-leadership responsibilities. One faculty member argued that our teaching philosophy should seek to provide graduates with tools that can be applied in their assignments immediately following graduation. One teaching method put forth in *The Adult Learner* was the use of adult learning models as the guiding process in seminars.[6] The other was based on *Education for Judgment*.[7] The faculty member decried the practice of providing students with multiple frameworks and theoretical perspectives without first giving them tools to use in the "real world." He asserted that not allowing students the opportunity to apply the perspectives to case studies was a waste of time given his perception of theoretical discussions with limited or no application.[8] With passion, the faculty member commented that such discussions could be purely academic exercises that would argue distinctions without differences. This contention caused us as educators to revisit the assumptions of adult learning or andragogy:[9]

- Adults have the need to know why they are learning something.
- Adults learn through doing.
- Adults are problem-solvers.
- Adults learn best when the subject is of immediate use.

In a larger forum, the debate continued on what our approach should be—to provide a framework with an application of the concepts presented in each of the lessons or to present multiple frameworks so that students would have a broad understanding of the topics. The battle lines seemed drawn superficially between faculty members with postgraduate educational experience and those with traditional operational "field" or functional experience within the military. It would be convenient but wrong to characterize the debate as "how to think" versus "what to think." The essential question faced by all faculty is how to teach "how to think" in the limited time we have in seminar. The USAWC faculty represents a range of educational and military experiences (it is a mix of civilian academics and predominantly military Active-duty and retired officers). With that in mind, our faculty members have preferred teaching styles for delivering our diverse curriculum.

Stakeholder Surveys

This is not a unique debate for us, or for educators writ large.[10] Our institution has explored this question through external and internal studies to determine the needs of future military officers and study approaches to educating military leaders for the 21st century.[11] Recent reviews of the USAWC curriculum focused on educating strategic leaders and educating strategic thinking.[12] Each study addresses presenting specific knowledge to develop competencies for near-term assignments—a pragmatic and rational approach to meet the short-term needs of the officers and their gaining organizations—as well as providing students with several tools that can be

Retired Ambassador Robert B. Zoellick, chairman of Goldman Sach's International Advisors, speaks to students, staff, and faculty during evening lecture at U.S. Naval War College, October 2014 (U.S. Navy/James E. Foehl)

useful in handling myriad situations. The goal is to develop within our graduates the ability to create their own ways to address the unforeseen circumstances in any environment.

Each study recommends that students receive a broad exposure to concepts that enhance development of their adaptive capacity—their ability to cope with a wide range of conditions. The Office of the Secretary of Defense study suggests future military leaders need "an appreciation for adaptability and flexibility. . . . Officers have to be comfortable with thinking in terms of the art of the possible. They must be able to take in multiple points of view and different perspectives."[13] However, some faculty members counter that students, as adult learners, need a tangible framework that can be applied to anticipated problems. The use of frameworks is commonplace in Army culture. Prior to senior Service schools, military education is based on standardized curriculum delivered uniformly. However, successful USAWC graduates must be able to determine when current doctrine is ineffective and then to develop new doctrine appropriate to the circumstances at hand. For example, our contemporary military experiences in Afghanistan and Iraq led to the development of a counterinsurgency doctrine that diverged greatly from the previous doctrine that focused on large-scale conventional operations.

Surveys of military leaders in operational and institutional positions have considered this educational issue. U.S. general officers reported that developing breadth of knowledge was more important for USAWC graduates than having depth of knowledge in specialized areas.[14] General officer respondents in 2012 indicated that USAWC graduates were well prepared to understand how to operate in the strategic environment, address and plan for the future while executing current missions, and deal with complex problems.[15] External observers and employers of our graduates suggest that a broad education with exposure to many perspectives enhances their adaptability as senior leaders.

Nonetheless, some students and faculty perceive the need to provide graduates with more specific ways to overcome both the predictable and unpredictable challenges of their next assignments. This can be accomplished by providing them with different frameworks or models that explain organizational phenomenon (descriptive) and also expose them to various approaches to accomplish organizational goals (prescriptive). If a tested theory becomes widely accepted, the resulting model is adopted to provide predicable results. However, when we can only rely on competing theories, each of which may describe the organizational phenomena for only certain conditions, then it becomes imprudent to assume that a single framework will suffice. Our recent graduates are best positioned to validate this assertion.

Our USAWC students, by virtue of their past successful performance and high potential, have been selected to serve in higher levels of the national defense establishment. They have real-world experience within their organizations that they can bring to bear on the issues that arise in their seminars. As an institution, we must convey the relevance and utility of the material we teach to our students who are archetypal adult learners.

Our military educational mission mirrors that of a public administration educational program. For this kind of education, Patricia Shields reminds us of the tradition of classical pragmatism. She discusses the applicability of the "four Ps": practical, pluralism, participatory, and provisional.[16] Our USAWC should likewise be *practical* by demonstrating the link between theories and our students' broad experiences. The diversity of our constituents as well as the interdependence of policy and decisionmaking systems reveals *pluralism* in the realm of national security. Developing a clear understanding of the problem space and potential solutions requires the *participatory* engagement of all members of the national security enterprise. Lastly, adopted policies are rarely "best" permanent solutions given the changing nature of the environment. In our realm, all policies and practices are *provisional.*

This reflection on USAWC education began with a forceful nudge by colleagues to examine how we should attempt to educate our USAWC students. I came to realize that we are faced with several paradoxes: We must educate both broadly and deeply. We must not only expose them to proven ways to address known challenges but also enhance their ability to adapt and create their own tools for new situations. We must encourage students to share their experiences while helping them view situations through different lenses. Each of these paradoxes presents a challenge to our faculty, who want to fully equip our students for the future while enabling them to perform effectively in their next assignment. One colleague called this "educating for certainty." But we must acknowledge that we are unable to do that. The future provides both continuity and change. So our educational approach should account for both and prepare our students to operate in the strategic landscape they will encounter.

A portfolio approach may be the most pragmatic way to meet our institutional goals. The portfolio curriculum design and materials offers established frameworks and theories combined with opportunities to explore emerging theoretical constructs. During a visit to USAWC seminars, a noted journalist and military historian challenged our students to use their year as "an opportunity to get bigger." Through historical examinations, he discerned that successful military leaders had the uncanny abilities "to accommodate other opinions" and "to be open to other points of view." These abilities help inform "bigger judgments" that senior leaders have the responsibility and obligation to make.

I realized that we as faculty must also accept the challenge to get bigger and move away from our own areas of comfort. We have to accept that we may not always have the right answer to provide to our students to solve problems that have yet to materialize. In designing courses and lessons, we should bridge the gap between preparing students for their next assignment and preparing them for their roles in an uncertain future. Some lessons will lend themselves to a tried and true framework and allow students to test their understanding of its concepts and applications in a case study. Even then, we faculty must encourage students to challenge even approved solutions. There will be other lessons where tried and true is not a viable approach and may even be counterproductive. These are better addressed by working through multiple perspectives. Faculty members who are responsible for specific lessons must keep in mind the deliverability of the lessons by the collective faculty and to the students. The overarching goal is to provide our graduates with the best possible preparation for future service to the Nation through this educational experience.

Implicitly, this goal must be sought at each of the DOD professional military education institutions, whereby its attainment will support success of the joint force. With the persistent challenges in the joint, interagency, international, and multinational environment, it is doubly important that the Armed Forces resist the pull of parochialism in the face of policy and fiscal uncertainty. Successful graduates of joint professional military education programs will have learned "how to think" and pragmatism in collaborative planning and execution of operations to support national security interests.

These reflections are intended to prompt the public administration and leadership education communities to also reflect on how to assist the U.S. military in its functions and responsibilities. The breadth and depth of research in these fields offer knowledge and practical applications that can be useful in national security matters. Further engagement and collaboration—a conversation—between the public administration, leadership education, and defense communities would benefit all. JFQ

Notes

[1] Donald F. Kettl and James W. Fesler, *The Politics Of The Administrative Process*, 3rd ed. (New York: CQ Press, 2005).

[2] Jeffery A. Weber and Johan Eliasson, eds., *Handbook of Military Administration: Public Administration and Public Policy* (London: CRC Press, 2007).

[3] Elihu Root, "The Army War College, Address at the Laying of the Cornerstone, Washington, DC, February 21, 1903," in *The Military and Colonial Policy of the United States, Addresses and Reports by Elihu Root*, ed. Robert Bacon and James B. Scott (Cambridge, MA: Harvard University Press, 1916), 121–129.

[4] Christopher Argyris and Donald Schön, *Organizational Learning: A Theory of Action Perspective* (Reading, MA: Addison-Wesley, 1978).

[5] Peter Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization* (Boston, MA: Currency, 1990), 14.

[6] Malcolm S. Knowles, Elwood F. Holton, and Richard A. Swanson, *The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development*, 6th ed. (San Diego: Elsevier, 2005).

[7] C. Roland Christensen, David A. Garvin, and Ann Sweet, eds., *Education for Judgment: The Artistry of Discussion Leadership* (Boston: HBS Press, 1992).

[8] Louis B. Barnes, C. Roland Christensen, and Abby J. Hansen, *Teaching and the Case Method*, 3rd ed. (Boston: Harvard Business School Press, 1994).

[9] Knowles, Holton, and Swanson; Peter Renner, *The Art of Teaching Adults: How to Become an Exceptional Instructor and Facilitator*, 10th ed. (Vancover: Training Associates, 2005).

[10] Frans-Bauke van der Meer and Arthur Ringeling, "An Education Strategy for Practitioners in Public Administration Master's Programs," *Journal of Public Affairs Education* 16, no. 1 (2010), 77–93.

[11] "The Military Officer in 2030: Secretary of Defense 2003 Summer Study," slide presentation (Newport, RI: Office of the Secretary of Defense, 2003); and William T. Johnsen et al., "The Army War College: Educating Strategic Leaders in an Age of Uncertainty," in *The Future of Military War Colleges*, ed. Jeffrey D. McCausland (Carlisle, PA: Dickinson College, December 2005), 22–185.

[12] Harry R. Yarger and Charles D. Allen, *Educating Strategic Leaders: Report of the Elective Program Review Working Group* (Carlisle, PA: U.S. Army War College, 2007); and Harry R. Yarger, *Educating Strategic Thinking in JSOU* (Washington, DC: Joint Special Operations University, 2007).

[13] "The Military Officer in 2030: Secretary of Defense 2003 Summer Study."

[14] *2012 U.S. Army War College General Officer Survey* (Carlisle, PA: U.S. Army War College, 2012).

[15] Ibid., 1.

[16] David H. Brendel, *Healing Psychiatry: Bridging the Science/Humanism Divide* (Cambridge, MA: MIT Press, 2006); and Patricia M. Shields, "Rediscovering the Taproot: Is Classical Pragmatism the Route to Renew Public Adminstration?" *Public Administration Review* (March/April 2008), 205–221.

Officer Candidate School instructor explains objective of teambuilding exercise including Marine Corps leadership traits, decisionmaking, and ethical leadership to students from University of North Carolina, at Marine Corps Leadership Seminar, April 2013 (U.S. Marine Corps/Megan Angel)

Vertical and Horizontal Respect

A Two-Dimensional Framework for Ethical Decisionmaking

By George H. Baker, Jr., and Jason E. Wallis

Everyone wants to be a good person; at least that tends to be a fundamental assumption about most of the people we work with in the Department of Defense (DOD). Yet the newspapers are frequently filled with articles about officers, enlisted members, and civilians falling from grace. Why do so many people make bad choices?

The dictionary defines *ethics* as "an area of study that deals with ideas about what is good and bad behavior: a branch of philosophy dealing with what is morally right or wrong."[1] This article proposes a simple two-dimensional framework for ethical decisionmaking. We kept it simple so it can be remembered. We believe this framework will

George H. Baker, Jr., is a Professor in the College of Distance Education at the U.S. Naval War College. Master Chief Jason E. Wallis is the Director of the Navy Senior Enlisted Academy.

be helpful throughout the day-to-day moments that sometimes challenge our professional ethics.

Vertical Respect and the Choice Continuum

This first part of the framework has its roots in a 1924 speech given by Lord Moulton in Great Britain. John Fletcher Moulton was the Minister of Munitions for Great Britain at the onset of World War I.[2] In what came to be titled *Law and Manners*, Moulton talked about a continuum of choices ranging from total freedom on one end to total restriction on the other. (Moulton used different terms, but the meaning is essentially the same.)

On the one hand, with total restriction the individual has no choice but to comply. Think of this as externally imposed obedience. One image that comes to mind is a prisoner complying with the orders of a prison guard. On the other hand, with total freedom there are no rules. People are free to do as they please. In Moulton's words, this realm "includes all those actions as to which we claim and enjoy complete freedom."[3]

Together, total restriction and total freedom represent the ends of a continuum of choice. Yet Moulton's speech was not about the ends of the continuum but rather the gray area of decisionmaking that lies between. Moulton called this gray area "obedience to the unenforceable."[4] Said differently, if total restriction is the realm of what we "must do," then somewhere beyond total restriction is the realm of what we "should do." In Moulton's words, obedience to the unenforceable "is the obedience of a man to that which he cannot be forced to obey. He is the enforcer of the law upon himself."[5] Behavior here is reflected in the old cliché, "it is what we do when no one is looking."

It is here that we take a slight departure from Moulton's original concept. The "choice continuum" relabels Moulton's obedience to the unenforceable as obedience to the (seemingly) unenforceable. Furthermore, obedience to the (seemingly) unenforceable often carries a sense of what we "might get away with"—for example, exceeding the posted speed limit. However, behavior today is often far more transparent than it was when Moulton first gave his speech. Modern-day transparency warrants associating Moulton's obedience to the unenforceable with what we call the *red zone*. In the red zone we have choices. For example, we all should obey the posted speed limit, right?

In his paper "Ethics in the U.S. Navy," Rear Admiral Ted Carter described Moulton's obedience to the unenforceable as "the sphere where individuals must exercise discretion and judgment, making decisions when the only enforcer is themselves."[6] Carter emphasized that decisionmaking in the red zone "relies upon an internalized sense of responsibility and an intrinsically-developed ethical core."[7] In other words, the red zone represents where one's true character comes to light. Do we consistently choose service above self?

We all make choices in the course of carrying out our duties. Some choices are ethical and others are not. Rather than emphasizing right and wrong, the Joint Ethics Regulation describes *ethics* as "standards by which one should act based on values" and *values* as "core beliefs such as duty, honor, and integrity that motivate attitude and actions."[8] As one might expect, the Joint Ethics Regulation is "applicable to all DOD employees, regardless of military or civilian grade."[9] The Joint Ethics Regulation goes on to say that "not all values are ethical values (integrity is; happiness is not)."[10] The unspoken message is to subordinate personal interests to organizational interests (that is, service above self). Making choices that are consistent with organizational values demonstrates vertical respect.

People who consistently make good ethical choices are said to be of good moral character. In his book *Education in the Moral Domain*, Larry Nucci defined *morality* as "knowledge of right and wrong. Conduct is moral if it involves selection of particular courses of action that are deemed to be right."[11] Again, the theme of choice takes center stage. Nucci posited: "The central feature of human morality is our capacity for choice and judgment."[12] Finally, Nucci concluded that "a person of good character is someone who attends to the moral implications of actions and acts in accordance with what is moral in most circumstances."[13] In other words, people of good moral character have the habit of making choices based on ethical values.

To summarize, the choice continuum considers three things: the individual, the situation, and the available choices. For DOD members, the heart of the choice continuum is in demonstrating vertical respect—making choices that reflect the values of DOD as embodied in the profession of arms. If there is any use at all in the choice continuum, it is in its ability to highlight the red zone, where individuals may be tempted to make choices based on personal interests at the expense of organizational interests. After all, everyone wants to be good, but sometimes we can benefit from a little reminder.

Theory to Practice: Life in the Red Zone

The DOD *Encyclopedia of Ethical Failure* is a readily available source of cases involving red zone decisionmaking. Here, the Standards of Conduct Office publishes a selection of cases for use in DOD ethics training. The Office cautions, "some cases are humorous, some sad, and all are real. Some will anger you as a Federal employee and some will anger you as an American taxpayer."[14] They all reflect individuals making choices in a given situation where obedience to organizational rules (that is, vertical respect) was seemingly unenforceable—at least to them.

Members who rise within the DOD hierarchy accumulate both responsibility and authority. Authority brings with it control of resources. The two examples that follow from the *Encyclopedia of Ethical Failure* illustrate bad choices by individuals in the red zone:

Your Posters Are My Posters. *An Army officer was convicted both for making false statements, including false statements in his confidential financial disclosure report (failure to report an outside position and the income from that position), and for*

Johns Hopkins University student tries to lower tensions during ethical decisionmaking field exercise at The Basic School (U.S. Marine Corps/ Emmanuel Ramos)

stealing government property. The employee put in an order at the department print shop, certifying that a series of posters were for official business. The posters were actually for the employee's side business. Additionally, the employee purchased a conference table, for which his own business got a $400 credit toward a conference table of its own. The employee was sentenced to 2 years of probation, 6 months house arrest, a fine of $25,000, and was ordered to pay $1,600 in restitution.[15]

Sampling of Gift Not Sufficient. *A lieutenant colonel committed dereliction of duty when, in violation of the Joint Ethics Regulation, he received a bottle of Ballantine's 30-year-old Scotch valued at $400 and failed to report it and properly dispose of it. In lieu of a court martial, the colonel resigned from the military service for the good of the service under other than honorable conditions.*[16]

In the first case, the Army officer abused his official position for personal gain. Following the explanation of ethical versus nonethical values from the Joint Ethics Regulation, we see that the Army officer chose personal happiness over integrity. In the second case, the lieutenant colonel also chose personal happiness over integrity by accepting a gift while in an official capacity and failing to follow the rules for doing such. In each case, individuals had to choose between what they "should do" and what they "might get away with." Unfortunately, they chose the latter.

One does not have to be senior to make bad decisions in the red zone. Take, for example, the use of government vehicles. Many in DOD, including those in the lower ranks or grades, have access to government vehicles. The rules regarding the use of government vehicles (including government-provided rental cars) can vary depending on whether one is at a permanent duty station or on temporary duty (TDY). Generally, government vehicles are for official use only. However, what constitutes "official" use can vary from one situation to the next. For example, using a government vehicle to make a burger run is permissible while on TDY, but not so while at a permanent duty station.[17] Thus, use of government vehicles is an area where government employees must be knowledgeable and careful of the rules. Beyond the area of government vehicles, many in DOD at

Johns Hopkins University student reasons with warlord of Centralian Revolution Army during ethical decisionmaking field exercise at The Basic School (U.S. Marine Corps/Emmanuel Ramos)

all levels hold U.S. Government credit cards, which carry their own list of dos and don'ts.

As members of the government in general and the DOD in particular, we hold a public office. We serve, and the public trusts us to serve ethically. The red zone is called the red zone for a good reason: it represents a danger area where normally good people have the opportunity to make bad choices. Bad choices in the red zone jeopardize the public trust enjoyed by all members of DOD. The choice continuum highlights the need to think clearly when making decisions in the red zone.

Bystanders play a role in the red zone, too. Just as a single candle can light the dark, sometimes all it takes is a single voice of reason to highlight the right choice—the right way ahead.

Although the choice continuum has value in promoting ethical decisionmaking relative to organizational values, it has some significant limitations. It covers only one dimension in decisionmaking—respect amid an organizational hierarchy (that is, vertical respect). The choice continuum is focused on *rules*, not on *relationships*. Although one might argue that "relationship to others" is already a part of the choice continuum, it is not obvious. This is where the second dimension of our proposed framework comes into play. Where "rules" and "choice" are the cornerstones of the choice continuum, "relationship to others" is the foundation of *domain theory*.

Horizontal Respect and Domain Theory

If ethics is the philosophy of right and wrong behavior, then morals frequently refers to what is "considered right and good by most people."[18] Good behavior is moral behavior, whereas bad behavior is immoral. Furthermore, moral issues often center on person-to-person behavior.

Domain theory in ethics considers the social standards of right and wrong in how we treat others. Dr. Larry Nucci begins his discussion of domain theory by drawing a distinction between morals and social conventions. Where ethics considers issues of right and wrong, "conventions are arbitrary because there are no inherent interpersonal effects of the actions they regulate."[19] Nucci provides the following example taken from an interview with a child to illustrate his point:

Figure 1. The Choice Continuum

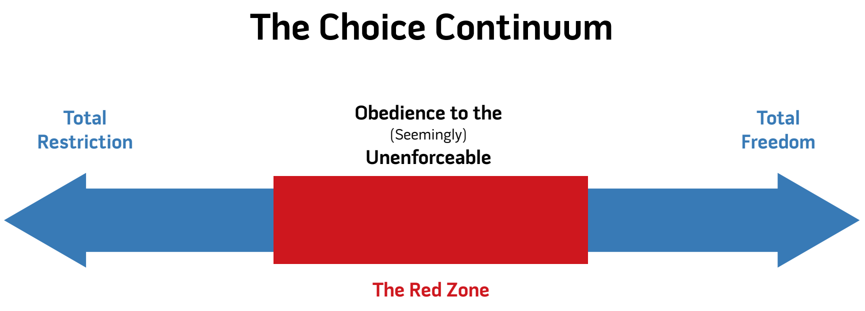
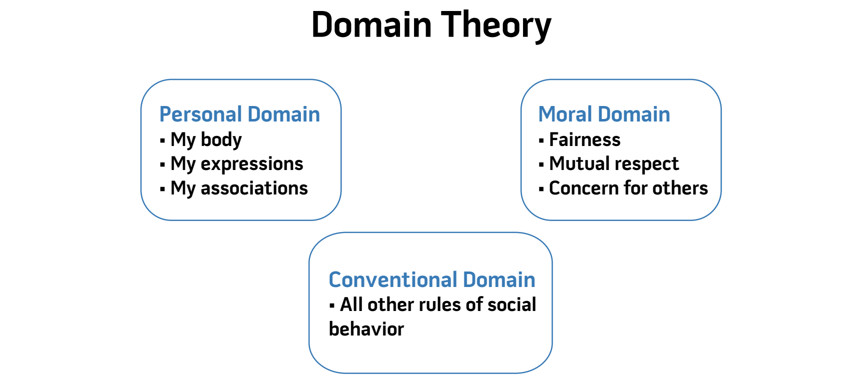


Figure 2. Domain Theory



Moral Issue: *Did you see what happened?* Yes. They were playing and John hit him too hard. *Is that something you are supposed to do or not supposed to do?* Not so hard to hurt. *Is there a rule about that?* Yes. *What is the rule?* You're not to hit hard. *What if there were no rule about hitting hard, would it be alright to do then?* No. *Why not?* Because he could get hurt and start to cry.

Conventional Issue: *Did you see what just happened?* Yes. They were noisy. *Is that something you are supposed to do or not supposed to do?* Not do. *Is there a rule about that?* Yes. We have to be quiet. *What if there were no rule, would it be alright to do then?* Yes. *Why?* Because there is no rule.[20]

In sum, the primary difference between moral and conventional issues is that the former carry an implication of potential harm to others.

Nucci further elaborates that moral issues are matters concerned with "welfare and physical harm . . . psychological harm . . . fairness and rights . . . and positive behaviors" toward others.[21] He argues that moral issues are independent of social norms. "Judgments of moral issues are justified in terms of harm or fairness that actions would cause, while judgments of conventions are justified in terms of norms and the expectations of authority."[22] Nucci concludes that "the core of human morality is a concern for fairness and human welfare."[23] In other words, domain theory has a powerful focus: social relationships—"the very ability of people to get along with one another."[24] Said differently, where the choice continuum centers on *vertical respect* (or respect for the institution), domain theory centers on *horizontal respect* (that is, respect for one another).

There are three domains in domain theory. The first is the personal domain. As Nucci explains, this is the realm "of the individual's identified freedoms."[25] The personal domain consists of "one's body and the claims to freedom of expression, communication, and association."[26] These are the personal rights of people to be individuals of their own designs, that is, to be whom they choose to be.

However, claims to individual freedom incur shared moral obligations. After all, exercising the freedom to be ourselves assumes that others grant us the freedom to do so. This give-and-take relationship is what Nucci labeled "*moral reciprocity*, mutual respect, and cooperation."[27] He argues, "Moral discourse transforms individual claims to freedom into mutually shared moral obligations."[28] In simple terms, through the principle of reciprocity the personal domain begets the moral domain. Nucci labels the moral domain as the sphere of interpersonal issues "pertaining to justice, human welfare, and compassion."[29] In other words, the moral domain comprises the "principles of fairness, mutual respect, and concern for the welfare of others."[30]

The third and final domain in domain theory is the conventional domain. It consists of all other rules that stem from living in a society, that is, "the agreed-upon uniformities in social behavior determined by the social system in which they were formed."[31] These are also the rules that are exemplified within vertical respect.

The conventional domain is vast and its rules are numerous. And as Nucci cautions, those rules are often changing and always relative to the society in which they were created. If the aforementioned cases from DOD's *Encyclopedia of Ethical Failure* were viewed through the lens of domain theory, they would fall within the conventional domain.

Lastly, Nucci makes an important point regarding the conventional domain. Where rules may come and go within the conventional domain, the rules in the personal and moral domains are few and enduring, giving a sense of permanence to this part of domain theory.

Horizontal Respect: Theory to Practice

One issue regarding horizontal respect gaining significant attention in today's military is sexual assault. In a December 2014 news conference, former Secretary of Defense Chuck Hagel told reporters:

> *Sexual assault threatens the lives and well-being of both the women and the men who serve our country in uniform. It destroys the bonds of trust and confidence, which* [are] *at the heart of our military. Eradicating sexual assault from our ranks is not only essential to the long-term health and readiness of the force, it is also about honoring our highest commitments to protect our fellow Soldiers, Sailors, Airmen, and Marines.*[32]

Similarly, the DOD 2014 Quadrennial Defense Review (QDR) states: "Eliminating sexual assault is one of the Department of Defense's highest priorities."[33] Using domain theory as a lens, we see that sexual assault is a violation of the moral domain, where mutual respect and concern for the victim's well-being are superseded by the perpetrator's selfish desires. In simple terms, sexual assault violates horizontal respect.

Another issue mentioned in the QDR is the urgency to implement changes needed "to fully realize [DOD's] decision to allow gay men and women to serve openly in the military."[34] Using domain theory as a lens, these are items of the personal domain—personal rights of expression and association. Again, these are items of horizontal respect.

Just as they did in the choice continuum, bystanders too can play an important role by speaking up when witnessing violations. Pulitzer Prize winner Robert Coles defines *moral leadership* as "a willingness to say and do what needs to be expressed."[35] He further argues, "This is one of the hallmarks of a leader—having the courage to speak up despite others' moods or discouragement."[36] Coles concludes that "what happens when moral values are really put to the test, when someone has to 'take the lead' in life,"[37] was moral leadership in action. With this definition in mind, the issues of sexual assault and of integrating gay men and women into the military will be solved only by people whose character reflects moral leadership.

To summarize, the strength of domain theory is its ability to highlight horizontal respect—our ability to get along with each other. By accepting our own personal freedoms, we incur an obligation to allow others to also realize their personal freedoms via the principle of reciprocity.

Framework Conclusion

Chapter 12 of the Joint Ethics Regulation lists 10 ethical values all DOD employees should consider when carrying out their duties. The first four deal with attaining vertical respect. They are honesty, integrity, loyalty, and accountability. The next five deal with horizontal respect. They are fairness, caring, respect (for others), promise-keeping, and responsible citizenship. The final value listed, pursuit of excellence, charges DOD members to be examples of excellence and to "strive beyond mediocrity."[38] This final attitudinal value is designed to maintain the public trust. Though it uses different words, the message in the Joint Ethics Regulation is clear. Members of DOD are expected to exhibit both vertical and horizontal respect.

Our goal was to come up with an ethical framework that could be useful in everyday decisionmaking. The concepts of vertical and horizontal respect seem to capture just that. Vertical respect is explained via the choice continuum, which highlights choices made in the red zone that are inconsistent with our values as members of the Department of Defense. Domain theory highlights horizontal respect and human relationships. Professionalism means integrating vertical and horizontal respect as we execute our duties, even at the expense of self-interest. Together, vertical and horizontal respect represent a practical framework that can illuminate better choices in ethical decisionmaking. JFQ

Notes

[1] *Merriam-Webster Online Dictionary* (2015).

[2] John Fletcher Moulton, "Law and Manners," *Atlantic Monthly,* July 1924, 1–4.

[3] Ibid., 1.

[4] Ibid.

[5] Ibid.

[6] Walter E. Carter, Jr., "Ethics in the U.S. Navy," U.S. Naval War College, March 24, 2014, 9.

[7] Ibid.

[8] Department of Defense (DOD), DOD 5500.07-R, *The Joint Ethics Regulation*, including Changes 1–7, November 17, 2011, 118.

[9] Ibid., i.

[10] Ibid., 118.

[11] Larry P. Nucci, *Education in the Moral Domain* (New York: Cambridge University Press, 2001), 4–5.

[12] Ibid., 112.

[13] Ibid., 124.

[14] Standards of Conduct Office, *Encyclopedia of Ethical Failure* (Washington, DC: DOD, October 2014), 3.

[15] Ibid., 70.

[16] Ibid., 82.

[17] DOD, Joint Travel Regulations, April 1, 2015, O-7.

[18] *Merriam-Webster Online Dictionary.*

[19] Nucci, 7.

[20] Ibid., 8.

[21] Ibid., 10.

[22] Ibid.

[23] Ibid., 19.

[24] Ibid.

[25] Ibid., 73.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid., 50–51.

[30] Ibid., 51.

[31] Ibid., 7.

[32] Tyrone C. Marshall, "More Must Be Done to Eliminate Sexual Assault, Hagel Says," DoD News, December 4, 2014.

[33] *Quadrennial Defense Review 2014* (Washington, DC: U.S. Department of Defense, 2014), 7.

[34] Ibid., xii.

[35] Robert Coles, *Lives of Moral Leadership: Men and Women Who Have Made a Difference* (New York: Random House, 2001), ix.

[36] Ibid., 7.

[37] Ibid., 226.

[38] *The Joint Ethics Regulation*, 118–119.

U.S. military and Japan Self-Defense Forces personnel engage in missile defense planning during Integrated Air and Missile Defense Wargame V, February 2014 (U.S. Air Force/Nathan Allen)

Waffles or Pancakes?

Operational- versus Tactical-Level Wargaming

By Dale C. Eikmeier

Ask people what the difference is between pancake batter and waffle batter,[1] and some will quizzically return the question, asking if there is a difference; after all, the batter looks the same. A few might acknowledge some differences but not know exactly what they are. Experienced chefs, however, will tell you the difference is the amount of eggs and oil in the batter. You can put pancake batter in a waffle iron and waffle batter on a griddle and both will cook, but the products will disappoint, especially if you were expecting crispy waffles or fluffy pancakes.

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

Wargaming at the operational and tactical levels is a lot like waffle and pancake batter: it might look the same and share many of the same ingredients, but it has important and subtle differences. Ask military planners what the difference is between operational-level and tactical-level wargaming methodologies used in course of action (COA) analysis, and you will probably get the same pancake-versus-waffle–type answers, with many telling you that the difference is nonexistent or not important. The truth is the wargaming processes may look the same, but the "ingredients" and outcomes are very different. Using a tactical-level wargaming focus at the operational level can result in the direction of well-planned and synchronized tactical actions at questionable operational tasks and the aiming of mismatched capabilities at ill-defined effects that fail to achieve operational and strategic objectives.

Many planners agree that operational-level wargaming using the Joint Operation Planning Process is different from tactical-level wargaming using the Military Decision Making Process or the Marine Corps Decision Process. But they struggle with understanding the differences because Service doctrines and joint doctrine describe only the processes and do not compare or point out differences between them. Not fully understanding the subtle differences, planners default to what they know best—which is usually the tactical level—and will apply tactical "pancake techniques" to the operational "waffle processes." This manifests itself when planners lose focus on the operational-level issues and drift toward trying to maneuver and fight functional or Service-component tactical actions rather than focusing on identifying and validating operational-level tasks. Planners can avoid this tactical drift only if they understand the difference between "tactical pancakes" and "operational waffles."

What versus *How*

The two wargaming processes are similar but not identical, and when things are not identical, the differences are important. The key difference between the operational- and tactical-level wargame is the type of questions and issues each focuses on. Simply put, the difference is a focus on *what to do* versus *how to do it* questions. This is important especially for operational-level planners because their level is the bridge that connects broad strategic guidance and aims toward tactical actions. That bridge is built out of *what* questions—what endstate, what effects, what objectives, what tasks, what capabilities—that are arranged with *when* and *where* questions. If operational-level planners do not understand this difference, they tend to wrestle with the easier and more concrete tactical *how* questions rather than the more difficult conceptual *what* questions. Operational wargaming asks, "Are we doing the right things?" Tactical wargaming asks, "Are we doing things right?"

The purpose of the wargame, at both levels, is to collect information to determine the advantages and disadvantages of each COA when compared to an evaluation criteria.[2] The operational-level COA and its wargame analysis are largely concerned with identifying and arranging the right endstates, objectives, effects, and tasks, along with matching the tasks to capabilities and resources in the correct sequence. These arrangements in time (when and sequencing), space (where), and purpose (goals) to achieve an endstate form the core of operational-level courses of action. Therefore, the operational level deals primarily, although not exclusively, with the *what* questions—what is the endstate, what objectives will achieve it, what effects must we create to achieve the objectives, and what tasks and action will produce those effects—and lastly the other *what* questions—when, where, and who will execute those tasks and actions. This is not to say there are no *how* questions at the operational level, but they are secondary to the more critical *what* questions; if they are wrong, it does not matter how well tactical actions are executed. So think big *what* and little *how* at the operational level, but keep in mind both are present; the scale simply is tipped toward *what* questions.

The tactical level is concerned with how to achieve assigned missions and objectives using the resources provided. Arrangements of unit capabilities in time and space to achieve effects and objectives form the core of tactical-level courses of action. Therefore, tactical-level wargaming deals primarily with the *how* questions: how are capabilities used, how are they brought to bear, how are they maneuvered, supported, and sustained. Like the operational level, the tactical level is also a continuum of *what* to *how* questions, but the scale at the tactical level is tipped toward the *how* side. So at the tactical level, think big *how* and little *what*.

Other Ingredients

The following discussion highlights some of the other important but subtle differences planners need to be aware of. These differences may be generalities, but they do represent key divergences between the two levels.

Aim. The aim of wargaming at the operational level, according to joint doctrine, is to determine the feasibility and acceptability of a course of action.[3] At the tactical level, according to Army doctrine, the aim is to refine, identify, analyze, develop, and determine key elements of the COA.[4] This doctrinal difference reflects some of the *what are we doing* versus the *how we are going to do it* approaches of operational and tactical levels. COA development at both levels uses the screening criteria of adequate, feasible, acceptable, distinguishable, and complete.[5] The tactical level, however, assumes that a COA has already met the screening criteria and that the aim of the wargame is to determine the *how to* details of the COA. The operational level does not assume the screening criteria have been met. With its focus on *what* questions, the wargame is the tool to determine feasibility and acceptability.[6]

Focus. The operational-level commander is concerned with identifying what to do, and the wargame helps validate the selection of objectives, effects, and tasks that will create the endstate conditions. The commander then resources, sequences, and synchronizes those tasks, and subsequently assigns those tasks to components. The COA is an arrangement of these elements, and the wargame helps determine if the arrangement will accomplish the mission and discern any advantages and disadvantages.

The tactical-level component or Service commander figures out how best to accomplish the assigned mission/task. Most of the *whats* have been determined and provided, so the tactical focus is on how to apply capabilities against them. The tactical-level wargame uses creative combinations of standard doctrinal schemes of maneuver, drills, techniques, and procedures against the situation.

Process. Both levels use the same action-reaction-counteraction model. However, there are slight nuances. The reaction in the tactical wargame is generally confined to the enemy and local population in the immediate area of operations, while the operational level considers the reaction of a broader community, including domestic and international audiences as well as adversaries.

Certainty. Operational-level planners may start with a blank sheet of paper and a vague directive to begin planning. They need to realize that some of their questions may be unanswerable at the time of planning or have no answers at all. Therefore, operational-level planners must be comfortable with higher degrees of ambiguity and working with a greater number of assumptions. While details and specifics are desirable and planners should work diligently to obtain or produce them, their absence cannot be an excuse not to plan.

Tactical planners, while also working in ambiguous environments, normally have the benefit of an operational- or higher level plan or planning guidance, which has attempted to reduce ambiguity, on which to build detailed plans. They should strive to reduce uncertainty and put as much detail as possible into tactical plans.

Method. The methods described in doctrinal manuals include the timeline analysis, critical events, and phasing of joint doctrine and the belt, avenue-in-depth, and box procedures of wargaming.[7] These methods are all temporal or spatial variations and offer options on which actions to wargame. The main differences between these methods are scope and detail. The operational level is larger in scope, broader and less specific on details, and makes more assumptions. It is a macro approach that focuses on doing the right things at the right time and leaves fine details of execution planning for component planners. The tactical level is smaller in scope, more specific and detailed, and strives to turn assumptions into facts. It is a micro approach that places importance on the details of how to execute the tasks and accepts that the operational planners correctly selected and assigned the tasks.

Media. Both levels use maps and matrices. However, the operational level's primary focus on *what* questions and the arrangement of objectives and tasks to capabilities, resourcing, and sequencing are generally more suited to a matrix supported by a map. The tactical level's primary focus on *how* questions deals more with schemes of maneuver, ranges, and time-distance relationships and is more suited to a map supported by a matrix.

Purpose and Outcomes. The purpose and outcomes are essentially the same at both levels: to generate and collect data so that advantages and disadvantages, strengths and weaknesses can be determined and used in COA refinement and the comparison process.

Elements of Power. The generally accepted elements of power are diplomatic, informational, military, and economic. The operational level considers all the elements in the development and analysis of COAs and is the primary integrator and synchronizer of the elements. Therefore, the wargame considers all the elements. The tactical level can consider all the elements, but it focuses mainly on military execution. At the tactical level, the other elements of power to be considered generally are environmental factors. Unless otherwise tasked, the tactical level leaves the integration or synchronization of the other elements to the operational level.

Participants. Because the operational level considers all the elements of power and synchronizes, coordinates, and occasionally integrates them, it is normal to include some unified action partners in the wargame. Unified action partners include interorganizational representatives, multinational forces, and nongovernmental and private sector organizations.[8] If a unified action partner cannot participate for security reasons, a responsible subject matter expert should replicate its actions, reactions, and counteractions. The inclusion of unified action partners (other than military) can occur at the tactical level, but it is the exception rather than the norm.

Higher Authority. The approving higher authority at the operational level will include military and/or civilian political leaders and possibly multinational organizations. Their guidance can tend to be broad, vague, and open to interpretation. At the tactical level, the higher authority, with few exceptions, is a military organization. Its guidance tends to be direct, specific, and less subject to interpretation.

Time-Space Factors. Time-space factors at the operational level help define the realm of possibilities, which are often defined by logistics and force structure. The operational level uses these factors primarily to determine the approximate sequencing of tasks. However, estimates of these factors are generally rough figures for a number of reasons. Exactness and precision at the operational level during planning are rarely possible, and there are too many variables and decisions to be made. In addition, the pursuit of precision can be counterproductive it if wastes time and results in rigidity. For example, an estimate that it takes *x* days to destroy an enemy capability may be sufficient for wargame purposes. Attempting to know the exact number of assets and amount of time required moves the operational-level planner to a tactical level that has not yet been planned. The tactical level attempts to use precise time-space factors for the synchronization and execution of operations because it is wargaming the actual execution of a specific assigned task.

Number of Levels Down. Army doctrine recommends wargaming two levels down; while joint doctrine does not explicitly state two levels down, it does hint at it.[9] This reflects the difference in the amount of detail necessary at the operational and tactical levels. Both look two levels down in practice, but they are looking at different things and asking

Soldiers provide covering fire for platoon during assault on enemy position during wargame exercise at Fort Bragg (U.S. Army/Michael J. MacLeod)

different questions. The operational level looks for the correct assignment of tasks to components one level down and asks whether the component has the correct capabilities two levels down to achieve the assigned task. The primary questions asked are who has the task and whether they have the resources or capabilities to accomplish it. Resourcing the right capabilities at the right time is the operational level's primary focus; how the capabilities are used is secondary. The tactical level looks at how the subordinate one level down will use assets two levels down to accomplish the task. Using capabilities is the tactical level's primary focus; resourcing them is secondary.

The processes of wargaming at the operational and tactical levels are similar but not identical, and it is the differences that become important. The key difference is a primary focus on questions of *what* at the operational level and questions of *how* at the tactical level. Planners, especially at the operational level, need to fully understand the differences. The operational-level wargame strives to determine if we are doing the right things and creating the right effects. The tactical-level wargame strives to determine the right way to accomplish the right thing. Not recognizing these differences can result in the wrong things done right, just like putting pancake batter in a waffle iron. **JFQ**

Notes

[1] Credit for the pancake/waffle analogy goes to Dwayne Wagner, Command and General Staff Officers Course Instructor, Fort Leavenworth, Kansas.

[2] Joint Publication (JP) 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011), IV-27.

[3] Ibid., IV-29.

[4] Field Manual (FM) 5-0, *The Operations Process* (Washington, DC: Headquarters Department of the Army, March 2010), B-32–B-33.

[5] JP 5-0, IV-24–IV-25; FM 5-0, B-15.

[6] JP 5-0, IV-29.

[7] Ibid., IV-32; FM 5-0, B-26.

[8] JP 3-0, *Joint Operations* (Washington, DC: The Joint Staff, August 11, 2011), I-8.

[9] JP 5-0, IV-30; FM 5-0, B-31.

An Interview with Christopher C. Bogdan

On May 12, 2015, Dr. William T. Eliason, Editor in Chief of *Joint Force Quarterly*, interviewed Lieutenant General Christopher C. Bogdan, USAF, Program Executive Officer for the F-35 Lightning II Program, at Bogdan's office in Arlington, Virginia. Erin L. Sindle transcribed the interview.

JFQ: Most critics of the F-35 start with the cost of the program. What did you and Assistant Secretary of the Navy for Research, Development, and Acquisition Sean Stackley recently tell Congress about the state of the program and this issue of cost?

Lieutenant General Bogdan: We said that costs are stable and actually coming down. When we look at cost, we look at three different areas. First, the cost of finishing the development program; and we have not asked for a penny more than what we were given in 2011 when we re-baselined the program. We believe that we're going to finish the development program without asking for any more money. The second piece is the cost of producing the airplane; and the price of buying the airplane has continued to come down. We think that trend will continue. In fact, we've set a target (delivered price per aircraft) for 2019 that when we sign the contract for those airplanes in 2019, we're looking for an airplane with an engine, with fee in then-year dollars, to be $80–85 million per F-35.

It's important that I give you those three caveats (aircraft, engine, and fee) because sometimes industry likes to report without the fee, which is just the cost. Sometimes the airframe guy likes to report his cost without the engine, and a lot of times they like to report the anticipated cost of a delivered F-35 in 2019 in base-year dollars, like FY12. We think we can get to an $80–85 million aircraft. So from a production point of view, we think we have a good understanding of the costs and what the drivers are to bring those costs down.

The big number is the O&S—the operations and sustainment cost. That's an estimate and, unfortunately, in this program it's a 50-year estimate; and it's an estimate that includes 2,443 U.S. airplanes. So by anybody's measure, that's going to be a huge number; and that's what gets people taken aback when we talk about the O&S cost of the F-35 program. That's where we get the "T" word—the trillion-dollar number. That number doesn't mean a whole lot to me. What I care about is what are we doing today in this program—concrete things—to drive that cost down, and are we seeing the results? The answer is yes. The bottom line is since 2011 we've dropped that estimate down 13 percent, and the CAPE [Cost Assessment and Program Evaluation] came in last year and did its own independent cost estimate of the O&S costs, and it validated that from 2011 to 2013 we dropped 9 percent. But the real issue is what are we doing now to reduce future O&S costs. We started a full-blown reliability/maintainability program, and we started a so-called "war on cost" room where we actually put the industry guys in along with some of our consultants and the program office folks. Any idea on how to reduce costs gets vetted. We look at return on investment and what it costs to invest; we look at the payback time; we look at how long it will take to implement; the team comes to the front office once a quarter and we decide on which things we will invest in and then adopt those improvements. We start taking concrete action today to drive down costs later. We think that by about the 2021 timeframe, we can at least get an A-model (U.S. Air Force version F-35) within 10 percent of the cost per flying hour of an F-16. (That's the best apples-to-apples comparison because the current F-16 cost per flying hour is a standard measure for operating costs of military aircraft.) Right now, despite what people think, that curve is coming down pretty nicely and we clearly understand in the program office that there are a lot of skeptics out there; we understand that the only way we can change minds is by showing them results. The words don't mean much—the results mean everything. Relative to cost, I would say we understand the three areas of development, production, and O&S. They're stable, and in those key areas we're doing things to drive them down.

JFQ: When you speak to public audiences about the program, how do you describe the capability of these weapon systems compared to current or legacy aircraft, both U.S. and foreign made?

Lt Gen Bogdan: I concentrate primarily on two attributes that this airplane brings, and I listen to what warfighters say and what they believe are game changers. The first of these game changers is the notion that a pilot can fly this airplane into complex, heavily defended areas and be survivable. The survivability comes about because of a combination of three aircraft characteristics: stealth, speed, and sensors.

Second, when this airplane is working right, it is extremely smart. It has multiple sensors that absorb lots of information, and then it can fuse that information to give the pilot a picture of the battlespace that is clear, concise, and accurate. It can also do that in places where the airplane remains virtually undetected. The pilot can get into a battlespace, see things, and then leave. That kind of situational awareness is not only important for the

F-35, but it's important for the rest of the weapons systems around the F-35. When we connect with them, it makes them and all those around the F-35 that much smarter and more survivable.

JFQ: How has the program evolved since you arrived as its Deputy Program Executive Officer and later moving up to lead it?

Lt Gen Bogdan: My predecessor came in and re-baselined the program because it had run off the rails. Vice Admiral David J. Venlet did a great job of putting some realism into that new baseline, and he brought some credibility back into the program. I picked up the ball, and now we've been executing—and we've been executing pretty well. Schedule-wise, we haven't missed a major milestone. We are still on track for Marine Corps IOC [initial operating capability] this summer and Air Force IOC next year. We are also on track to meet partner and FMS [Foreign Military Sales] deliveries in the future.

Another aspect of the program that is accelerating is the building of a global sustainment enterprise. This is a major undertaking. There are some additional complicated undertakings for which the program is responsible that I am sure people are unaware of in this area. For example, we're building two factories other than just the one at Fort Worth to build this airplane; we're building a factory in Italy and a factory in Japan to fabricate and check-out F-35s. For the engine, we're also building a factory in Turkey and another in Japan. We are also building a supply, repair, and heavy maintenance capability in both Europe and the Pacific regions—just like the one we are building here in North America. Creating a global sustainment enterprise with 14 different customers across 3 regions of the globe is a very, very complex task.

From a fundamental level, since I took charge I've tried to institute four different principles in the way we do business here, and I think if we get these four right, we've got a better shot at succeeding.

Lieutenant General Christopher C. Bogdan, USAF (U.S. Air Force/Andy Morataya)

First and foremost, the most important principle is integrity. You've got to run the program with integrity—and that starts with me. My team knows that we always do things with integrity so people believe us and we remain credible because the program runs on trust. We tell people the truth whether it's good, bad, or ugly, and we don't spin things.

The second principle is transparency. When you're spending the kind of money we are spending and you're the biggest program in DOD [Department of Defense] history and you've got 14 customers who are depending on you, you had better bet your bottom dollar that people are going to want to know what's going on. For us, transparency is a way of life. Every decision we make, every dollar we spend, we'd better be ready to stand up in front of whomever and tell them what we did and why we did it. Whether it's the parliament of a partner nation, whether it's Congress, whether it's the press, or OSD [Office of the Secretary of Defense], people need to know what we're doing and why we're doing it so they can continue to have trust in what we're doing.

The third principle is accountability. Accountability in one direction is easy. The program office is going to hold the contractor accountable—this is a simple concept to understand because that's what people expect, that's what's built into our job title in the program office. What's a lot harder with accountability is holding yourself accountable and holding the rest of the enterprise and stakeholders accountable because if you're not careful, your stakeholders and the people who have an influence on this program can do some pretty bad things to it despite their best intentions. So we preach 360-degree accountability. We make commitments, we hold ourselves accountable to those commitments, but we make sure everyone else in the enterprise also recognizes that they have to be held accountable to their commitments also.

Finally, the last principle is discipline. We don't have the time or the money, and the enterprise doesn't have the patience anymore for us to have to do things over again. We just can't have "redos." The way you can avoid do-overs is with discipline up front. You've got to start things with discipline and then you've got to keep that discipline throughout—even if it might take you a little bit longer initially—because in the endgame it won't take you longer if you get it right. It will take you a lot longer if you have to redo it.

With those four principles, no matter what program you're running, if you have those in place and you have your team operating and behaving that way, you probably have a better chance of success.

JFQ: A number of earlier issues were widely reported in the press, each seemingly difficult to solve, such as the specialized flight helmet. Are any of these issues showstoppers in terms of meeting your planned schedule? If so, which ones and how are you dealing with them?

Lt Gen Bogdan: That's a great question. If you'd taken a snapshot of the program 3 years ago, I could give you a list of four or five technical things that were always in the front of everybody's mind. We had a problem with the hook on the C-model; it couldn't catch the cable. We had a problem with the helmet, which had glow problems, "jitter" problems, and stability problems. We had problems because the plane couldn't fly in lightning. We had problems when we released fuel out of the wing dump system; fuel would stick to the bottom of the wing and migrate into panels in the fuselage. We also had reliability and maintainability problems.

Here's what I can tell you today. Every one of those problems is either solved or on the path to being solved. So for us, the measure of a good program is not zero problems; the measure of a good program is having problems, making discoveries, and solving them—and you solve them in a way that keeps the program on track. But now a different set of problems is in the headlines. Last year we had an engine problem that created a fire on the airplane. Guess what? We have all of that taken care of. Production engines are now being built with new pieces and parts so that won't ever happen again. We are retrofitting the entire fleet with new parts as well. So with that engine anomaly, which was a significant negative event on the program, we got to the root cause, we got to the solution, and we implemented the solution.

What's not behind us yet is software—there are more than eight million lines of code on this airplane. That's about four times as many as on legacy airplanes. Offboard, the systems that surround the airplane—mission planning, reprogramming, ALIS [Autonomic Logistics Information System]—contain *twice* that amount of software. If we don't get software right on this program, we're going to be in big trouble. That's number one. Number two is our Autonomic Logistics Information System (ALIS), which is a heck of a lot harder than anybody ever thought. We treated the ALIS system early on in this program like a piece of support equipment. It's not; it's way more complicated and important than that. It's the brains and blood of operating this weapons system. It has the maintenance information in it. It has the logistics information in it. It has the airplane configuration in it. It has all of the training for the maintainers and the pilots in it. It talks to the ordering systems when it needs parts. We fielded an airplane—long before ALIS was mature—and that ended up putting a lot of stress on the maintenance guys out in the field.

We treat ALIS today as if it were its own weapons system with an engineering discipline, software metrics, testing, design reviews—all the stuff we lacked years ago. From my perspective, there are always going to be problems. There are going to be things you don't know about now but you're going to know about later. The mark of a good program is that you can get over them.

The last problem I will share with you is the structural integrity of the B-model, which has cracked in places where we thought it might from the models, but more severely than we thought it would. There are a couple of reasons for that. The first reason goes back to early in this program when the B-model went through a weight-reduction. It was thousands of pounds overweight. One of the ways we took weight out was to reduce the thickness of a lot of the structure. We also switched from titanium to aluminum on a number of structures, which is lighter, but not as strong. That has come back to haunt us a little bit. We went through a significant event last year when we cracked the main bulkhead on the B-model. We thought it could crack, but when it did, it transferred loads to a bunch of the other bulkheads and they cracked too. So we have been working for over a year to come up with a newly designed bulkhead, which we now have in production for lot number 9. We also are trying to get a process known as laser shock peening qualified on the airplane. This process can reinforce and strengthen the crack-prone areas of the bulkhead without adding weight and without having to tear apart the bulkheads.

JFQ: As the largest customer of the aircraft, what does the U.S. Air Force think about the F-35A's ability to meet all the missions it expects it to perform, particularly close air support [CAS]?

Lt Gen Bogdan: The part of the dialogue that has been missing about the CAS mission is that we are delivering CAS capability in two increments. We designed the program so that in the initial years, it wouldn't have all its capability; it's incremental. Will F-35 be a good CAS airplane by 2018? You bet. But it's not there yet. It will have a gun,

Captain Brent Golden, 16th Weapons Squadron instructor, taxis F-35A Lightning II at Nellis Air Force Base, January 2015 (U.S. Air Force/Siuta B. Ika)

and that gun will work, but it's not the only thing we use in the CAS mission. It will be used in conjunction with other capabilities such as precision-guided munitions. It will have the right kinds of communications systems to work with ground forces. Eventually in Block 4, we'll have full-mission video. The jet already has incredible sensors, so at night and in inclement weather you have the same capabilities as daytime. I think it's a little unfair when folks who have an affinity for other airplanes in the CAS role compare those aircraft to an F-35 without acknowledging that the F-35 can do so many other things that those aircraft cannot do beyond the CAS mission. When you build a multirole airplane, it's probably not going to be a superstar in everything it does, but it's going to do a lot of things really well. And, when you compare the F-35's survivability, sensor fusion, and the situational awareness it brings, you have an excellent weapon system.

JFQ: Can you talk about the international portion of the program and how that has evolved?

Lt Gen Bogdan: There's a much deeper relevance to the international part of the program, and I'll start first with the partnership itself. There are nine partners in the program when you count the United States as a single partner; so we have eight other partners, with most of them in Europe. The only two not in Europe are Canada and Australia. The first important piece about the partnership is that the partners get a say in what happens with this program, and for some of them, that experience of being part of a big and complicated airplane acquisition program is a great lesson for them. Also, we have all eight of our other partners' personnel in the program office who work as part of the program—another great learning experience for them and for us.

There are two other important aspects of the partnership. First is the ability for our partners to be able to fight alongside us as equals and be able to use the same ROEs [rules of engagement] because their airplanes, pilots, and maintainers are just as capable as we are. This means they can also lead in the hardest missions. The last piece has to do with the fifth-generation technology and our partners' industries participating in the program. We're providing technologies that we expect our partners to protect, just like we would. So, in one sense, we're requiring them to upgrade their security infrastructure to a level beyond what they may already have. Also, many partner

F-35B Lightning II Joint Strike Fighter taxis on flight deck of USS *Wasp* during night operations as part of Operational Testing 1 (U.S. Marine Corps/Anne K. Henry) industries involved in the program are getting an opportunity to understand and be part of modern manufacturing techniques and advanced technologies and are being asked to hold themselves to a pretty high standard if they want to be suppliers on this program. From the DOD's perspective, a stronger, allied industrial base gives us future access to better technologies and also pushes U.S. industry to get better.

JFQ: News media reports have mentioned an increasing number of cyber attacks being conducted against the Defense Department in recent years. What impact has this growing threat of cyber attacks had on your program's ability to deliver a capability that can effectively deal with these cyber-related concerns?

Lt Gen Bogdan: When we talk about cyber threats to this program, we talk about them in two different environments. The first environment is the infrastructure we use to design, develop, sustain, and field the airplane; for example, the F-35 IT system we use to pass program and design information among the partners, services, and program office. From this perspective, I have the utmost confidence in the protections the Department of Defense has put in place for those IT systems. We still have to remain extremely vigilant when it comes to industry's systems. In the past, this is where we have found vulnerabilities in the F-35 program. Consequently, DOD and industry have worked together to increase the protections we put in place to prevent F-35 information from getting into the wrong hands. Each and every day we're feeling a little bit better about both government IT and industry IT systems. I say this because a number of times every year multiple agencies—to include [U.S.] Cyber Command and 22nd Air Force—visit the F-35 program and do penetration and vulnerability testing. Not of the airplane and the weapons system, but of our IT systems. So from that perspective, they are truly helping us by showing us what we need to do to make ourselves more resilient, robust, and secure.

Now let's talk about the airplane and the weapons system itself. Without getting into details, what I will tell you is if you know from the beginning of a program you will be exporting the weapon system—and you want to hand it to allies to let them operate it in their own environments—you can, from the start of the program, build in the appropriate protections. This is one of the first airplanes that I know of where at the start of the program we consciously knew it would be an exportable weapon system. Therefore, from a design and architectural standpoint, one of the upfront requirements was to protect the critical technologies of the weapons system. That is pretty powerful when you start from the beginning because you don't have to adapt, you don't have to strap things on, you don't have to make what I would consider to be secondary or tertiary changes to protect things. As a result, it has what I would consider to be a very strong built-in protection scheme.

JFQ: What challenges and risks do you see for the program ahead and what will you recommend your successor focus on?

Lt Gen Bogdan: From a technical and performance standpoint, I think we will be able to solve any problems we encounter. We have to think about continuing to evolve the airplane to meet future threats. The good news is the architecture of the airplane was built such that it has growth potential. We're working toward things like open-systems architecture for sensors. We have already done our first upgrade of all the major computers on the program and are planning another upgrade in about 4 or 5 years. So from a technical standpoint, I would tell my successor to keep an eye on the need to make the weapon system more open. In addition, I would tell my successor that from a business perspective I think we're starting to get costs under control, but we must continue to take deliberate actions now to drive down future costs. The real big thing that's still out there is building what I call the global sustainment enterprise. If you think about where we're going to be in 10, 15, or 20 years, we'll have 2,000-plus airplanes out there, located all over the globe and being flown by at least 14 customers. We are trying to build the support and sustainment system to take care of all those airplanes. We're building depot and heavy maintenance capabilities in the Pacific and Europe just like we have here in the United States. We are creating a global supply chain; we are creating a global network of repair capability in all 3 regions. All of this is not fully built or mature yet. Over the next 5 to 7 years the person who comes next is going to have to take that onboard full steam because our partners and FMS customers will have aircraft in operations soon. We're adding 17 operating locations in the next 5 years and almost half of them are overseas. We've got to be ready to have a global sustainment structure in place and ready to operate. We're on a really tight timeline to get that done for our partners and Foreign Military Sales customers. They expect that the day they get their airplanes in country, all the infrastructure they need to support the weapon system will be in place and ready to go: supply chain, repair chain, maintenance manuals, training systems, etc.—all of it. That's big. From that perspective, it's probably where the focus really needs to be in the next 5 years.

JFQ: Would you recommend future weapons systems that meet similar requirements for multiple Services be managed by a joint program office such as this one?

Lt Gen Bogdan: First, if the warfighters and customers are willing to compromise with each other on the requirements, joint programs can work. Our history of joint programs is such that they don't work very well—not only because of the lack of compromise but because we've also thrown on some mismanagement. When you put those two together—folks who weren't willing to compromise with their requirements along with a program that doesn't have those management and leadership fundamentals down pat—you've got a train wreck coming. We've

Navy test pilot flies F-35B Joint Strike Fighter aircraft BF-3 with inert AIM-9X Sidewinder missiles over Atlantic Test Range (U.S. Navy/Courtesy of Lockheed Martin/Michael Jackson)

seen that in the past and the result is that the program dies or is split up along Service lines.

Congress has asked me this same question a number of times. If you would have tried to develop an A-model for the Air Force, a B-model for the Marine Corps, and a C-model for the Navy as separate programs, I think you would have probably run into similar problems, but the solutions and cost and time required to implement those solutions would have been a unique Service problem versus a partnership problem. The advantage this program has over three separate programs is that there are huge economies of scale to be had: for example, global supply pooling (where one part can service many customers) or multiple repair facilities around the world can be very effective and efficient. If you're a U.S. Marine Corps B-model deployed in the Pacific and something goes wrong with the airplane, you can get a part or repair in the Pacific theater from a partner or FMS customer. From that perspective, I think the program has an advantage over a single-Service program. But joint programs are hard to manage. They tend to be riskier for all the reasons discussed compared to single-Service programs, but the rewards are greater if you can get it there.

Additionally, in this austere budget environment, the Department and Services must share technology, not duplicate effort, and build airplanes that can adapt and do many things. Adaptability is very important. If we're going to keep airplanes around for 30 or 40 years, you'd better start building them so they have growth potential and adaptability.

JFQ: Is anything you would like to add that we have not discussed?

Lt Gen Bogdan: The biggest issue I would like your readers to understand is that this is not the same program it was years ago. We had some really rough times in the past, and I think the Department, the partnership, and industry have begun moving this program in a better direction. We're not there yet, but like a large ship, it takes a long time to turn . . . but it is turning. I would ask people to judge the program on the progress it's made since the re-baseline and not look in the rearview mirror. **JFQ**

Civilian Expeditionary Workforce member engages local business owner in discussion regarding poultry feed production, Kandahar Province (Kentucky National Guard/Dallas Kratzer)

Turnaround
The Untold Story of the Human Terrain System

By Clifton Green

The U.S. Army's Human Terrain System (HTS), a program that embedded social scientists with deployed units, endured a rough start as it began deploying teams to Iraq and Afghanistan in 2007.[1] These early experiences had a lasting impact on the program. Although critics have written extensively about HTS struggles with internal mismanagement, most accounts simply cataloged problems, yielded little insight into the organization's progress over time, and ultimately gave the impression that HTS was never able to make needed corrections. Far from being a failure, though, HTS is a remarkable turnaround story and should serve as a case study for how organizations can implement fundamental organizational changes. Even more importantly, the reformed version of HTS provides

Clifton Green is a Human Resources (HR) Business Partner at the Department of Health and Human Services. Previously, he was an HR Manager and Advisor with the Human Terrain System.

Human Terrain System member speaks with Afghan during Key Leader Engagement in Kandahar Province to discourage locals from hiding contraband for Taliban (DOD/Crystal Davis)

a template that could significantly improve existing Department of Defense (DOD) support to deployed civilians, thousands of whom have provided critical services to war-fighters around the globe.

History

Inception to Government Transition. HTS was developed as a response to concerns about mismanagement of U.S. military operations in Iraq and Afghanistan, in particular the lack of cultural understanding of these countries demonstrated by the U.S. military. Soldiers, commanded by leaders with limited cross-cultural experience, were being asked to navigate a complex foreign environment with little or no training, and they were failing.

Prior to U.S. involvement in Iraq and Afghanistan, cultural research and analysis had only a small place in the Army thought process. HTS changed that. Designed to provide a better understanding of indigenous populations in these countries, it was hoped that HTS would help U.S. and allied forces reduce violent misunderstandings and dampen the insurgencies. In 2006, the Army, facing progressively worsening situations in Iraq and Afghanistan, needed new ideas and thus backed a $20 million, five-team HTS proof of concept. Even before all five teams had been deployed, early reactions from theater commanders were favorable. Within a year, the requirement for Human Terrain Teams mushroomed to 26 teams as the price tag surpassed $100 million annually.

In the mad dash to fill positions, HTS hiring standards ranged from minimal to nonexistent. In many cases, new employees were not even interviewed. When combined with high starting salaries, this lack of selectivity caused HTS to attract a peculiar mix of highly qualified personnel, absolutely unqualified personnel, and everyone in between.

As the number of workers swelled at the HTS base of operations in Fort Leavenworth, Kansas, two distinct camps emerged. Army Reservists, with varying levels of military experience, formed one group, while contractors formed another. Although it is contractors who typically play a supporting role to government and military personnel, in the early days of HTS it was the military members who lacked a clearly defined role. The vast majority of deployed team members and support staff were contractors, while HTS acquired Reservists with no plan to integrate them. In some cases, military personnel battled the contractors for control, but the HTS support contract required that contractors administer most daily operations. This difficult situation was exacerbated by the fact that HTS's program manager and its contract oversight were both based a thousand miles away in Virginia.

To deal with these problems and provide better government oversight, a deputy program manager was appointed at Fort Leavenworth in late 2008. His role was to oversee the work of both contractors and military personnel. It was a difficult task. HTS's highly matrixed organization, internal rivalries, and lack of controls had created a dysfunctional work environment, which operated in an ad hoc manner in almost every way. Policies and procedures were virtually nonexistent, and most work was done by key employees with narrow areas of expertise. Mid- to senior-level managers were, in too many cases, absent or ineffective.

Some HTS managers who did work hard to address the program's problems were overwhelmed. When decisions were made, they were often inadequate to resolve the problem or simply too late to matter, and the staff required to implement the decisions was insufficient. Such problems were largely due to management officials who had difficulty navigating the unstructured work environment. Instead of establishing systems and frameworks to deal with problems, managers generally approached each problem as a unique circumstance. At the same time, the lack of structure enabled many employees to perform poorly and face few consequences. Without structure to regulate behavior, HTS employees often succumbed to a kind of organizational attention deficit disorder. This combination of factors created serious deficiencies for HTS quality of support.[2]

In late 2008, these problems were compounded by a new looming crisis. The United States and Iraq had signed a Status of Forces Agreement that put U.S. contractors working in Iraq within the jurisdiction of the Iraqi legal system. Panicked that Iraqi police (or insurgents masquerading as Iraqi police) might arrest employees, HTS initiated a plan to convert all 150 Human Terrain Team (HTT) members from contractors to government employees. To facilitate the process, a government transition assistant was assigned to manage the conversion from Fort Monroe, Virginia, with HTS designating several personnel to assist. All HTS team members had to become government employees by May 31, 2009, or return to the United States.

The conversion, which seemed simple in the abstract, quickly became a nightmare. HTS employees, a notoriously vocal workforce, were bewildered by the turn of events. They deluged the transition assistant with thousands of questions, complaints, and pages of paperwork, and productivity in theater declined while employees wondered about their futures and haggled for better terms. At the same time, numerous other issues, from travel orders to timesheets, required HTS to establish a large number of new internal processes. Like HTS managers, the transition assistant had no system to handle the volume and was quickly overwhelmed. As the situation deteriorated, it was unclear whether the deadline could be met, or if HTS would be forced to embarrassingly remove all personnel from theater.

Fortunately, through furious last-minute efforts by HTS and U.S. Army Training and Doctrine Command (TRADOC) staff members, the conversion process was completed on time. However, tremendous damage had already been done to HTS credibility, and dozens of employees (over one-third of the HTS deployed workforce) had quit. Bureaucratic infighting caused several staff principles, including the deputy program manager, to depart in mid-2009, and a large portion of the organization was suddenly moved from Fort Leavenworth to Virginia. Although HTS had survived the crisis, many inside and outside of the program began to question HTS's fundamental level of competence.

Wandering in the Wilderness. After the conversion debacle, HTS drifted. The decision to relocate several sections of the organization caused further division. At the same time, the lack of strong management limited the organization's ability to make necessary changes. Competing HTS staff elements struggled to fill the vacuum, resulting in a critical lost year.

In the middle of the conversion process, the HTS program manager created a Program Management Office–Forward (PMO-Forward) in both Iraq and Afghanistan in response to real problems, including the lost accountability of employees in a war zone. The role of the PMO-Forwards, however, was never clearly established, and HTS staff members generally viewed the PMO-Forwards as deployed staff elements. The PMO-Forwards, by contrast, considered themselves deputy program managers. Mutual mistrust inhibited collaboration, and a months-long standoff ensued. In spite of the need for internal cooperation, HTS program management never publicized or enforced clear guidelines for how the PMO-Forwards should interact with the staff. Staff meetings between PMO-Forwards and U.S.-based support staff devolved into uncomfortable stalemates. The ensuing discord severely restricted HTS capacity to improve support processes and fed into the HTS culture of dysfunction.

Once teams were staffed with government employees, HTS found itself poorly equipped to meet the needs of its workforce. Contractor-to-government transition planning had been exclusively focused on the conversion process; little preparation had been made for actually supporting government civilians. As contractors, HTS personnel had been supported by corporate human resource (HR) and finance sections, but now those organizations were out of the picture. While regulations and support agencies already existed for government civilian HR and finance issues, those agencies were unequipped to deal with the range and complexity of issues presented by HTS employees.

HTS needed experts to create processes and integrate systems. Lacking both, the newly formed HTS HR Directorate was drowning in problems.

For instance, the HTS finance section was staffed by one timekeeper, a Soldier with no background in civilian finance. The lack of support caused the number of pay problems to snowball over time, damaging morale and productivity. Meanwhile, employees in theater had received virtually no training on proper pay practices and would regularly claim to be working in excess of 12 hours per day, 7 days a week. This led to real integrity problems for the organization. While the tempo of operations in theater was certainly high, reports suggested that not everyone was being truthful on their timecards. One team leader did implement significant restrictions on the number of hours employees could claim and was immediately hounded from theater—"fired" by a PMO-Forward who had no legal authority to fire anyone. With no one controlling payroll and a generally lawless atmosphere, team productivity was highly variable. Unfortunately, there is little doubt that some HTS employees took advantage of the situation to pad their timecards while doing little work (a practice that was regrettably common among deployed Federal workers in Iraq and Afghanistan, not just at HTS).[3]

HTS was simply not operating in accordance with established rules. However, with the government transition complete, it had inherited a rather large rulebook. At the same time, HTS often lacked clear lines of authority within its mix of military, civilian, and contract workers, all of whom were led by a program manager who served on an Intergovernmental Personnel Act agreement, an unusual employment arrangement that further confused matters. The lack of administrative clarity created an overall impression that HTS had no rules, and large numbers of disgruntled HTS employees soon found their way to the inspector general, various elected representatives, and Equal Employment Opportunity offices. Between late 2009 and early 2010, Congress had withheld tens of millions of dollars from the HTS budget and had directed the Center for Naval Analyses to perform an assessment of the program. Other investigations, including an Army Regulation 15-6 inquiry and an internal audit by the TRADOC Internal Review and Audit Compliance office, were bubbling up as well. HTS's flaws had become impossible to ignore.

Reform. Virtually every HTS employee acknowledged the need for change. The real question was what shape reform would take. Many wanted the program to simply break away from the intrusive rules and regulations, and believed that most problems could be solved if HTS left TRADOC, which they viewed as both unhelpful and adversarial, and moved to U.S. Army Forces Command or U.S. Special Operations Command. Others thought this analysis missed the point. In their view, HTS would have to adapt to the Army and to civilian employment law regardless of which command it fell under. Resistance was not only futile but also destructive and would only cripple the program. HTS would have to learn how to follow the rules.

This conflict had remained unresolved for most of the program's history. The HTS program manager had often made a point of emphasizing the program's uniqueness and claimed that this made HTS incompatible with the Army's existing bureaucracy. TRADOC, which provided oversight of HTS activities, represented that bureaucracy, and as a result was often perceived as an existential threat and met with hostility within HTS. This animosity was at times mutual. Many viewed HTS fiscal wastefulness and poor internal regulation as something of a threat as well, since it would be TRADOC—not the HTS itinerant workforce—that would be left to clean up after HTS failures. TRADOC managers also found HTS's grandiose plans, such as a training directorate with more staff than students, to be exasperating. These conflicting perspectives caused the relationship between the two organizations to sour over time, and TRADOC found itself confronted daily with the question of how much leeway to give HTS. With the United States engaged in two concurrent wars, there was no easy answer.

Nevertheless, several abortive efforts to clean up aspects of the program from within had taken place. Unfortunately, each had been hindered by a lack of expertise or a failure to follow through. While HTS had a large staff, most staff members were unaware of the mechanics of how the program functioned. The few "old hands" who understood the nuts and bolts of HTS typically tried to fly under the radar amid staff infighting. When ideas did coalesce into concrete proposals, HTS staff principals were generally unable to implement changes due to being overwhelmed by problems and uncertain of the second- and third-order effects of any proposed solution. HTS program management had done little to encourage organizational discipline of any kind. This created an environment largely free of formal consequences, such as reprimands or terminations, even in the face of egregious behavior. To become more legally compliant and effective, HTS would need to irritate many of its longtime employees, who had become accustomed to the consequence-free environment. Taking them on, however, risked pushback from both employees and other managers, so most managers found it safer to do nothing.

Because HTS was overseen by TRADOC G2 and had, over the course of several years, proved unable to effectively self-manage, TRADOC gradually took on a more active role. Unfortunately, the logistics of this relationship were problematic. Most of HTS was physically remote from the TRADOC G2 offices. TRADOC G2 lacked experience overseeing a program such as HTS, and it had both limited access to what was going on within the program and limited manpower. Additionally, HTS sometimes attempted to replicate TRADOC management functions within itself, creating confusion and making cooperation difficult. These factors prevented TRADOC G2 from being able to implement reforms unless HTS was an active and engaged participant. Unfortunately, because HTS leadership generally viewed TRADOC with suspicion, there was little in the way of productive dialogue.

In early 2010, a small group of HTS personnel and TRADOC G2 management officials operating out of

Fort Monroe, Virginia, began intensive work on overhauling the program's administration. The group had detailed insight into the workings of HTS and significant expertise in civilian HR and finance. Over the next few months, a number of policies covering a range of issues were drafted and sent to HTS program management for review. At the same time, the group received additional manpower and was able to improve payroll processing, eliminating a backlog of over 80 pay-related complaints that affected most deployed employees. Unfortunately, implementation of other policy changes was limited. Although the proposals provided a clear and legally compliant model for managing the program, they remained in limbo, neither approved nor rejected. The HTS program manager was simply not enthusiastic about institutionalizing the program.[4]

By mid-June 2010, the pressure of the investigations and HTS management's continuing resistance to reform brought the situation to a breaking point. Two key changes, however, appeared to signal a fresh start for the program. First, the position of program manager was eliminated. Second, an Active-duty Army colonel, who had previously served as the TRADOC Deputy G2 and was thus familiar with the HTS program and its difficulties, was named director. The new director had longstanding and positive relationships with TRADOC G2 staff members and thus understood how to balance the considerations of TRADOC with the goals of HTS. Most importantly, she was more pragmatic than her predecessor, who had generally declined to focus on day-to-day management issues.

Anxious to implement change, the HTS director gave the green light to a number of the policies drafted by the Fort Monroe group. The group also gained authority and leadership support in a number of significant areas, including program administration, program development, payroll, travel, hiring, and separations. These changes significantly improved efficiency, transparency, regulatory compliance, and internal controls.

Afghan girl peeks around door as U.S. Special Forces and Cultural Support Team speak with her father, Uruzgan Province (DOD/Kaily Brown)

New guidance documents eventually covered dozens of topics, and improved internal processes gave managers better insight into how well HTS was running. In addition, new HTS policies established a change management structure that allowed the program to continue to improve. Finally, more discipline was imposed on the hiring process, resulting in more accurate recruitment targets and 61 percent lower attrition in training.[5] As positive change continued, many employees expressed relief that HTS was finally turning a corner.

Not everyone agreed, however. For example, although travel privileges had been significantly misused, some supervisors were annoyed about having to ask for permission under the new, more accountable procedures. Timesheet reviews turned up cases of excess that, when addressed, created some hostility. The PMO-Forward positions, which lacked accountability to other staff elements, were abolished and replaced with the position of Theater Support Officer, which reported to the HTS director of operations.

While process improvements occurred rapidly, improving the HTS workforce took longer. Because HTS had been willing to hire almost anyone in the early days, it had a large number of unproductive employees. Other employees were competent professionals but had a contentious relationship with the program as a result of the years of mismanagement. By 2012, however, a combination of changes had significantly improved workforce quality. These included better management, the termination of more than a dozen employees, more stringent hiring criteria, and a requirement that most employees separate from HTS at the end of their deployment. Employees wishing to deploy again could reapply just like anyone else. This not only improved workforce quality, but it also enhanced the program's ability to fine-tune recruiting requirements. By 2013, terminations for cause had declined

Soldiers from Charlie Troop, 2-38 Cavalry, and DA civilians, Human Terrain System, with local Afghan villagers during Key Leader Engagement in Kandahar Province (DOD/Crystal Davis)

greatly, reflecting an increasingly stable and professional workforce.

Although HTS had made remarkable internal transformations, media coverage of the program was stuck in 2009.[6] HTS's most frequent critic, a blogger named John Stanton, had written numerous articles that reflected extensive employee disgruntlement and captured some of HTS's chronic mismanagement.[7] As things improved, however, critics either minimized or failed to notice the changes made in the program. While this may have been intentional, it seems more likely that they simply were not aware of what was happening. The HTS of 2009 was wide open to the media, a decision that did not serve the program well. To combat this, HTS post-2010 was more closed. Public relations and other outreach efforts continued, but other forms of openness diminished. At the same time, investigations into HTS's 2009-era failures were being broadly disseminated on the Internet. Even though the program had significantly improved, HTS critics had few ways of discovering this, as they received most of their information from public sources and disgruntled employees. Given the lack of information, they assumed that little had changed.

They were wrong. HTS had, in many ways, become an example of how to do things correctly. A 2013 external review pointed out progress toward institutionalizing the program.[8] Subsequent internal reviews, audits, and investigations conducted during 2013 and 2014 found an effectively managed organization that complied with regulations. This was verified by a comprehensive audit conducted by the Army Audit Agency in 2014. The HTS experience offers important lessons that can shape the way DOD deploys civilians during the next conflict. It also offers broader lessons about how to improve the government's employment practices.

Implications

Centralizing Support for Deployed Civilians. While poor management limited HTS during its early years, the program was also hindered by DOD's ineffective civilian deployment system. The U.S. military is capable when deploying uniformed Servicemembers, but its civilian deployment process is minimal and poorly integrated. For small organizations, or units with only a few civilians, this is a nuisance to be endured. For HTS, which deployed civilians at a larger scale, the system's weaknesses created massive challenges to mission accomplishment.

The effects were significant. The U.S. Government spent almost $800 million on HTS from its inception through the 2014 Afghanistan drawdown, a period of over 7 years. During much of that time, mismanagement, excess attrition, inflated salaries, and poor support practices wasted hundreds of millions of dollars. Furthermore, assuming HTS provided value to battlefield commanders, the years it took to fix these issues and field more effective teams may well have cost lives and worsened the outcomes in both Iraq and Afghanistan.

Some might argue that waste was an inevitable byproduct of the program's rapid creation in the middle of two conflicts. There is truth to that. However, if a civilian deployment infrastructure had existed prior to the creation of HTS, the program could have used it directly. Instead, HTS, like other programs that deploy civilians, had to figure everything out, build its own infrastructure, and endure numerous failures on the road to getting things right. That was a phenomenally inefficient way of doing business. It was also completely unnecessary.

DOD should establish a program to manage the recruitment, training, deployment, and sustainment of government civilian personnel in overseas environments. This centralized program would enable deployed forces to quickly obtain needed civilian skills to augment their capabilities. At the same time, it would allow programs and supported units to focus on core competencies rather than administrative distractions. Finally, such a program, by eliminating inefficiencies, could save the government hundreds of millions of dollars during future conflicts. While that may sound like an overstatement, the HTS experience demonstrates that cost savings of this magnitude are not theoretical.

While HTS provided civilian cultural expertise in Iraq and Afghanistan, future wars may require wholly different and unexpected types of knowledge. In the past, such needs were often filled through the contracting process. However, government civilians may be preferable to contractors for several reasons: they are more cost effective; they fall under the direct control of government authorities; and they can perform inherently governmental functions. In other cases, the use of contractors is unnecessary because the desired expertise already exists within DOD's permanent civilian workforce. This capability was previously leveraged through the Civilian Expeditionary Workforce (CEW) program, which provided opportunities for existing government civilians to deploy. Regardless of the source, though, experiences in Iraq and Afghanistan prove that such skills will be required.

Unfortunately, civilian personnel are often inadequately prepared to deal with the military deployment bureaucracy, which is focused primarily on military personnel and contractors. As an example, HTS employees who received care at military treatment facilities in theater would often be categorized as "contractors" simply because there was no option for "government civilian," creating unnecessary challenges to medical support. Civilians drawn from the private sector had even greater difficulty adapting to the military's way of doing business. These distractions made them and their organizations less productive and increased the amount of turnover. The HTS experience demonstrates that an entire program's operations can be hobbled by the investigations, negative publicity, and employee issues that accompany deficiencies in administrative support.

A centralized DOD civilian deployment program would provide support throughout the entire tour, from the receipt of notice to deploy through to the end of the deployment. Programs and units sending civilians downrange would use this program's centralized support capabilities and expertise. It would prepare civilians for deployment, ensure coordination with deployment centers and receiving units, account for them in theater, ensure a smooth redeployment home, and provide accurate administrative, finance, and logistical support throughout the entire process. It would also ensure that deployed civilians received proper assistance and care, while making certain they performed the work they were hired to do.

Such a program would need to accommodate itself to the reality of defense budget cycles, expanding and contracting as required. During peacetime, it could be sustained by a minimal number of employees; during wartime, it would expand by using limited-term government employees and contractor support. The program would serve individual deployers as well as large organizations and would centralize functions currently duplicated across DOD, paying for itself by eliminating waste. As a "one-stop shop," the program would encourage consistent support of deployed civilians while maintaining administrative best practices, reducing the amount of waste and fraud committed during deployments.

Naturally, there are always concerns about the use of government employees rather than contractors. First, government hiring is an extremely slow process. To circumvent this issue, HTS developed a hybrid contractor/government hiring process that utilized the strengths of the private sector to augment government hiring methods. Contract recruiters were able to find large numbers of potential candidates with needed expertise. The candidates were screened and their names were then submitted for government qualification. If qualified, the candidates attended a training class prior to being sworn in as government civilians. This approach allowed HTS to provide a volume of personnel that would never have been possible using normal government recruiting methods.

The second main issue with government workers is the concern that they become permanent employees who are difficult to remove from service. This is not the case. Term-limited appointments allow management to decline employment extensions as needed. Term employment thus makes adjustments to the size of the workforce relatively easy, avoiding the need for a reduction in force, and provides a mechanism to release underperforming employees while avoiding the difficult and emotionally draining termination process. Employment can end with the expiration of an employee's term rather than through termination, allowing the employee to save face and ensuring that he or she is able to file for unemployment. Unfortunately, however, termination can be necessary in some cases. At HTS, 18 employees were terminated over a 5-year period, a rate considerably higher than normal for the Federal Government. This was possible because of effective coordination between HR, supervisors, and program leadership. An effective civilian deployment program could provide supervisors with the necessary expertise to separate employees with performance or behavioral issues.

Clearly there is an unmet need to improve support for deployed civilians. While the CEW program performed some of the functions mentioned above, it was limited in scope and served mainly as a matchmaker, posting deployed positions that individuals could apply for. Although it filled a useful role, CEW did not provide the kind of "cradle to grave" support that is necessary for maximum workforce effectiveness.

DOD must act quickly to improve support before more institutional knowledge is lost. A 2012 Government Accountability Office report outlined how DOD neglected to learn from civilian deployment experiences in Bosnia, which led to costly and preventable failures in Iraq and Afghanistan just a few years later.[9]

Sadly, history seems to be repeating itself. In March 2014, the CEW Web site announced that the program would no longer provide a "sourcing solution for joint civilian requirements," and that this function would instead be performed by the Army G1.[10] (The remnants of the CEW program have since migrated to U.S. Army Central Command.) With drawdowns continuing, cuts to CEW were inevitable. Unfortunately, it appears that this migrated function, now renamed the International/Expeditionary Policy Office, will provide fewer capabilities than CEW did. A less effective organization is not the answer. Senior leaders must understand this challenge and recognize that supporting civilians properly is not just the right thing to do; it also improves effectiveness and makes sound financial sense.

Pay and Performance. Prior to the 2009 HTS conversion from contractor to government workforce, deployed team members typically made between $250,000 and $400,000 per year. While this rate of pay was not unusual for deployed contractors at the time, large salaries alone were not sufficient to recruit top-quality personnel for Human Terrain Teams. In some cases, team members lacked even basic social science and research skills. Despite these shortcomings, individuals were uniformly paid large salaries, with highly inconsistent results.

Over time, the salaries paid to HTS employees gradually diminished. After the government conversion, the salary range for HTS employees dropped to roughly $180,000–$300,000 per year. Not only was this less than they had made as contractors, but as government civilians every dollar of salary was taxable as well. (Contractor salaries enjoy significant tax benefits.) In addition, the team leader and social scientist positions that had been graded as GG-15 were reclassified as GG-14, cutting the top end of the salary range by another 15 percent.

In 2013, sequester restrictions forced Army commands to implement restrictions on overtime work for all employees, including deployed civilians. While these restrictions were not well enforced by many units in theater, TRADOC G2 implemented meaningful restrictions on overtime use. As a result, the average annual salary of a deployed HTS team leader, which had hovered around $400,000 in 2008, dropped to around $200,000 in 2014. Although HTS employees were generally displeased with these changes, support to deployed units remained consistent, and internal assessments showed that commander satisfaction remained high.

Despite this dramatic cost savings, there is no evidence that HTS employees in 2014 were any less capable than employees in 2008. While comparing the two periods is difficult due to the lack of verifiable metrics from 2008, deployed commanders and staff who responded to internal surveys in 2014 almost uniformly agreed that HTS products were relevant, aided decisionmaking, and added to the unit's sociocultural understanding of the environment. More importantly, HTS, which in the early years suffered a significant number of team implosions, mutinies, and cases of job abandonment, saw a substantial decrease in these types of incidents. Furthermore, while HTT members in 2008 often lacked basic competencies (human terrain analysts were sometimes considered suitable only for vehicle washing duties), by 2014 the average HTT member was significantly more capable.

How was HTS able to cut salaries in half and yet still achieve superior results? First, the exorbitant salaries of 2008 were simply part and parcel of the military's institutional culture at the time. With Congress appropriating hundreds of billions of dollars as part of the late war surges, budget discipline was significantly relaxed. Unfortunately, while those excessive salaries lured few serious academics, they did attract a wide variety of individuals who were more interested in cashing in than achieving the Army's goals. At the same time, HTS's no-rules internal culture imposed significant costs on supervisors who tried to conscientiously enforce restrictions. When HTS team members were contractors, the company lost money if personnel were not deployed and claiming long hours. At the same time, the HTS leadership team believed that it needed to fill teams at all costs. The incentives within HTS were strongly arrayed against any kind of internal restrictions, with all of the attendant disciplinary problems. As a result, HTS quickly earned a reputation as a haven for problematic personalities, which harmed future recruiting efforts and created a negative feedback loop.

Over time, as salaries shrank and regulations governing conduct increased, the greedy gradually departed. While this was a positive step, the large salaries set at the beginning severely limited the ability to hire employees at the proper wage. It also ensured higher program costs throughout the program's lifespan. While the excessive salaries of 2008 may have enabled HTS to build its workforce more quickly than it could have otherwise, it is unclear that employees obtained this way were worth having at all. The HTS experience demonstrates that high salaries are not necessarily beneficial for hiring and that they can be more destructive than helpful, both financially and operationally.

Process Defeats Politics. During its early years, HTS was an organization driven by personalities, not procedures. When difficult or unusual situations involving HTS employees arose (an almost everyday occurrence), staff members would many times quickly defer the question to the program manager, who was not physically present and likely would not make a decision. This was a symptom of HTS's broader challenge wherein the organization's decisionmaking process had failed to evolve in the face of rapid growth. Because the program had few policies or guidelines, even a minor variation to a routine procedure created decisional gridlock. As a result, every decision point became an opportunity for organizational politics or simple inertia to run the program aground.

To meet this challenge, HTS generated internal policies, an employee handbook, a pay and allowances guide, and more than a dozen internal "bulletins" that explained the nuances of complex issues such as workers' compensation and emergency leave. Because of the continuously changing nature of the HTS program, a fixed catalogue of policies would have been inadequate. Documents were thus revised as necessary to ensure that they remained relevant, sensible, and responsive. In addition, HTS policies were designed in such a way that they were not only enforceable, but would also actually be enforced. This proved crucial to making the changes work. Where possible, consequences were applied automatically rather than at the discretion of a manager. This limited accusations of favoritism and ensured fair treatment across the workforce.

As these reforms were implemented, some within the program argued that a policy-centric and enforcement-based approach was too heavy handed. Unfortunately, HTS's toxic environment required far greater articulation of the rules and far more comprehensive enforcement strategies than would ordinarily have been required in a program of its size. Employees, supervisors, leadership, and support sections all possessed limited faith in one another's abilities and motives. Additionally, the "short timer" mentality of many employees, a high turnover rate, and a lack of coordination all enhanced this lack of confidence. When employees asked a question and received an answer they did not like, they had learned to simply ask another decisionmaker until someone provided the desired answer. Leaders often had trouble saying no to reasonable-sounding requests that were, in fact, not reasonable. By establishing clear and enforceable written policies, HTS significantly reduced this deeply ingrained and disruptive pattern of behavior. Given the complexity of government personnel rules and the volume of turnover, merely establishing informal guidelines would not have been effective.

This approach benefited HTS in numerous ways. The amount of attention from management that was required to administer the program declined significantly because routine matters could be handled at a lower level. In addition, rather than having to bargain for everything, employees could review HTS policies and understand what they were and were not entitled to. As a result, when disgruntled employees disagreed with established policies and filed complaints, it was relatively straightforward to have the complaints dismissed. Finally, once the values animating those policies became entrenched, a cultural change took hold and HTS became a radically different place at which to work.

While HTS may be remembered for its chaotic early blunders, the program's later, quieter years demonstrate the effectiveness of its turnaround. Although the program may not survive in today's difficult fiscal environment, future sociocultural research efforts will likely be institutionalized in new and different ways. However, there does not appear to be any equivalent effort to improve DOD's poorly functioning civilian deployment system. It would be a shame to throw away $800 million worth of hard-won experience. After more than a decade of counterinsurgency and unconventional warfare, leaders must recognize the important role civilians will play in winning future conflicts. JFQ

Notes

[1] For a detailed account of Human Terrain System (HTS) history, see Christopher J. Lamb et al., *Human Terrain Teams: An Organizational Innovation for Sociocultural Knowledge in Irregular Warfare* (Washington, DC: Institute of World Politics Press, 2013), which is detailed, even-handed, and accurate. Unfortunately, it does have some blind spots, but this article fills in some of those.

[2] Ibid., 147. Lamb et al. reference three types of Human Terrain Team (HTT) members: "ne'er-do-wells," "fantasists," and "workers." While these categories are crude, they are also quite accurate. Within the HTS staff, the vast majority of personnel could be categorized as ne'er-do-wells or fantasists. Even if new arrivals did not begin their tenure with HTS in one of those two frames of mind, the environment tended to have a negative effect on those exposed to it. Workers were rare.

[3] It is important to note that timecard exploitation was routine for civilians in Iraq and Afghanistan. To HTS's credit, team members never approached the excesses of deployed Department of Justice employees, who often claimed to continuously work 16 hours per day, 7 days a week. See Department of Justice, Office of the Inspector General, *An Investigation of Overtime Payments to FBI and Other Department of Justice Employees Deployed to Iraq and Afghanistan* (Washington, DC: Department of Justice, 2008), available at <www.justice.gov/oig/special/s0812/final.pdf>.

[4] Lamb et al., 73–74.

[5] Based on decline in attrition from HTS training, from 2009 to 2013.

[6] Tom Vanden Brook, "Army Plows Ahead with Troubled War-Zone program," *USA Today*, February 28, 2013, available at <www.usatoday.com/story/news/world/2013/02/17/human-terrain-system-iraq-afghanistan/1923789>.

[7] John Stanton's articles were the product of numerous sources within the program, but were also largely based on second-or third-hand rumors. In many if not most cases, his specific allegations were inaccurate. However, his articles often did accurately reflect the tone of internal dissent within HTS.

[8] Lamb et al., 78–79.

[9] Government Accountability Office (GAO), *Afghanistan: Improvements Needed to Strengthen Management of U.S. Civilian Presence*, GAO-12-285 (Washington, DC: GAO, 2012), available at <www.gao.gov/products/GAO-12-285>.

[10] Department of Defense, "The Civilian Deployment Experience," available at <cpms.osd.mil/expeditionary/home.html>.

Army Rangers assigned to 2nd Battalion, 75th Ranger Regiment, prepare for extraction during Task Force Training on Fort Hunter Liggett, CA, January 2014 (U.S. Army/Steven Hitchcock)

On Military Professionalism and Civilian Control

By Carnes Lord

Recently, the subject of military "professionalism" has gripped the attention of top echelons of the Department of Defense (DOD) to a degree that is perhaps unprecedented. Most notably, Chairman of the Joint Chiefs of Staff (CJCS) General Martin E. Dempsey has directed each of the Services to review and rearticulate its understanding of the profession of arms in the context of its particular missions, traditions, and practices. Former Secretary of Defense Chuck Hagel signaled his own concern with such matters by appointing a two-star admiral as his special assistant for military professionalism and ethics. And at both the joint and Service levels, serious attention is starting to be given to improving and systematizing the way the U.S. military develops its leaders and communicates what it expects of them. In the discussion that follows, I focus on the issue of military professionalism in a broad joint or DOD perspective, leaving aside for the most part Service-related professionalism issues.

There are several proximate reasons for the renewed focus on military

Dr. Carnes Lord is Professor of Strategic Leadership at the Naval War College.

professionalism. A steady drumbeat of scandal has dogged the military in recent years: the Abu Ghraib abuses in Iraq, desecration of enemy corpses in Afghanistan, cheating on proficiency tests, personal corruption, and sexual misbehavior of all kinds. Particularly alarming is the widespread and well-publicized incidence in the military (including relatively senior ranks) of sexual harassment and sexual assault, which has resulted in intense political pressure on the military to take drastic steps to address this problem. At a more fundamental level, however, there seems to be a sense among Pentagon leaders that the demands of "the long war" have taken a psychological toll on our military—especially the Army and Marine Corps—that has contributed to a noticeable erosion of the traditional values underpinning the professional ethos of the Armed Forces.

Compounding these concerns is what can only be described as the continuing disintegration of traditional moral and cultural values in the larger society. The weakening of organized religion in much of the country, the breakdown of the family, the impact of Hollywood and popular music, and related developments pose a formidable challenge to the good order and discipline of a military that, thanks to the Internet and contemporary social media, is even more inextricably embedded in civilian society and culture than ever before. Our military leadership has for the most part resisted the temptation to blame bad behavior by the troops on the external environment ("the culture made me do it"). It is, rightly, sensitive to the danger of encouraging those in uniform to look down on their civilian counterparts. At a certain point, however, one wonders whether some hard choices will not have to be made in this respect. The Marine Corps has long recognized that the socialization of young recruits necessitates a certain countercultural stance toward American society.[1] The time may well be approaching when the other Services will have to follow suit if American military professionalism is to be sustained over the long run.

What is military professionalism? Surprisingly little serious thought seems to have been given to this question since Samuel P. Huntington's classic work *The Soldier and the State*, published more than a half-century ago.[2] Many seem to understand "professionals" as merely the opposite of "amateurs"—that is, people who are paid to do a job requiring a high level of competence and skill. (Like professional football players, so the joke goes, military officers are skilled at what they do and "look good in a uniform.") A recent survey of junior Army officers revealed considerable uncertainty and doubt as to the meaning of professionalism in that Service. One respondent claimed, "I know very few Army officers [who] consider [themselves] under the term 'professional' in the same category as doctors and lawyers." Some felt that Army professionalism had been degraded by various monetary incentives; others cited pervasive micromanagement and lack of trust on the part of senior leaders as factors undermining their professional status.[3] All of this is symptomatic of a larger problem extending throughout the Services: the creeping bureaucratization of the military establishment.

A government bureaucracy, like a traditional business corporation, is a hierarchical structure designed to maximize efficiency through highly routinized processes and behaviors. The military Services are and indeed have always been bureaucracies, with the pathologies inherent in such organizations. But the Services have also had a professional component that has served to limit and counteract the ill effects of bureaucracy. A key aspect of professionalism is institutional autonomy. The military art cannot be reduced to a set of routinized rules of behavior but requires independent or discretionary judgment and the intellectual and moral preparation to exercise it responsibly. By the same token, a true profession is self-policing in terms of recruitment, the setting of standards of competence, and promotion. Professionalism rightly understood serves a particular mission that the professional body alone has a socially recognized ability to perform. When professionalism is eroded by bureaucratization, the accomplishment of that mission has a tendency to take second place to the care and feeding of the organization and its individual members. At this point, professional pride tends to be eclipsed by a trade union mentality and loyalties become focused on the organization more than on the larger society it is meant to serve. When this happens in a military organization, the trust the broader society reposes in that organization is at risk and fundamental frictions in the civil-military relationship are likely to result.

In Huntington's well-known analysis, military professionalism is the key to healthy civil-military relations—what he calls "objective control" of the military by its civilian superiors. Under a system of objective control, the military is conceded substantial autonomy in the areas just mentioned in return for its respect for and noninterference in the decisionmaking of the civilian leadership. But this is possible only if the military is a professional one. By contrast, nonprofessional forces (for example, civilian militias) require "subjective control"—that is, direct and continuous involvement by the political authorities in managing them.[4]

It has to be said at once that the American experience has never been completely congruent with Huntington's objective control model.[5] But his argument about the importance of military professionalism for the civil-military relationship remains a fundamental insight. Since the end of the Cold War, some observers have called attention to what they believe to be signs of growing frictions, if not an incipient crisis, in civil-military relations in the United States. Others have expressed concerns over an alleged "militarization" of American foreign policy as exemplified in the increasingly important diplomatic roles of our regional combatant commanders. Whatever the truth of the matter (it is easy enough to argue that such concerns are sometimes grossly exaggerated), any rethinking of military professionalism today needs to be centered in these larger issues.[6]

Every profession must understand and accept its mission and the nature of the competencies that enable it to

Army Ranger sights target with M240L machine gun during company live-fire training at Camp Roberts, CA, January 2014 (U.S. Army/Teddy Wade) achieve the mission. These competencies are sometimes referred to in the relevant literature as "jurisdictions."[7] These jurisdictions are not necessarily stable but rather are subject to change over time, as the mission itself evolves in differing circumstances or other competing organizations vie for them. They are subject to negotiation and renegotiation both horizontally (with competing organizations) and vertically (with higher authority). In Huntington's study, the mission or jurisdiction of the military profession is famously said to be "the management of violence." This is clearly inadequate, both because it is too general (remember the professional football player) and because it is too narrow to account for all the competencies militaries necessarily (or often, or ideally) require. A more current term, subject to similar objections, would be *warfighting*.

There is a considerable lack of agreement and basic clarity about the current jurisdictions of the U.S. military, both within and outside its ranks. Perhaps most striking is the issue of "strategy." The U.S. military over the years has tended to be reluctant to take full ownership of strategy as a mission, and at times has seemed to abdicate it in favor of civilians (in the case of nuclear strategy or McNamaran systems analysis) or to higher authority (the State Department or National Security Council). It is sometimes suggested that the ascendency of operational art at the expense of strategy in current military parlance has been significantly motivated by an essentially bureaucratic desire to minimize civilian interference in the military sphere.[8] It is doubtful that any of the Services have really operationalized strategy in their personnel and education systems. There has been a proliferation of so-called strategy documents in the military and within the U.S. Government generally in recent years. Few if any of these have anything to do with genuine strategic thinking. Meanwhile, the performance of the American military and government at the strategic level in Iraq and Afghanistan over the last decade has clearly left much to be desired. Was this a failure of the military profession? If not, why not?

There is an obvious link between the orphaned condition of strategy in American national security policymaking and other jurisdictional arenas, which remain problematic and contested. The most important of these are counterinsurgency; postconflict stability and reconstruction operations; engineering and business expertise; language and cultural expertise; and the contracting-out of traditional military missions (for example, security in a war zone). Arguably, it is incumbent on a truly professional military to recognize the need to clarify and, where necessary, to re-adjudicate its jurisdictions. For the most part, the U.S. military does not seem to recognize this to the extent it should. One recent important exception is the doctrinal elevation of stability and reconstruction operations to the same status as warfighting as a military mission in the wake of our manifest failure to manage the postconflict situation in Iraq. It remains to be seen, however, what the operational realities of this move will turn out to be in the strategic environments of the future. This stands in stark contrast to the way the U.S. military establishment prepared for postwar governance and reconstruction during the later years of World War II.[9]

Another significant arena in which the tension between military professionalism and bureaucracy is evident is resource allocation. To the extent that the military seems to be dominated by Service parochialism in its search for funding rather than by an honest assessment of what is good for the military as a whole in achieving its mission, military professionalism is undermined. When this happens, civilian authority (Office of the Secretary of Defense, Office of Management and Budget, Congress) is likely to intervene in the process and impose its own solution, with significant damage to the autonomy of the military and the trust necessary to maintain it. Service parochialism will clearly never be completely eradicated. However, in spite of the mantra of "jointness," one can argue it is regarded by many in the military today with unwarranted complacency. The extent to which Service parochialism not only tarnishes public and congressional perceptions of the military but also sets a poor leadership/ethical example throughout the chain of command does not seem to be well understood.

A related issue central to military professionalism and civil-military relations is the ability and willingness of military leaders to "speak truth" to civilian power in supporting their independent military judgment. If the main interest of the leadership is protecting the military's bureaucratic equities, it will tend to develop a transactional relationship with the civilian hierarchy that mutes disagreement or challenges to policy in exchange for favorable treatment on matters of immediate concern to it. This was central to the failure of the Joint Chiefs to challenge wrongheaded civilian decisionmaking during the Vietnam War and perhaps more recently as well.[10] It is a fundamental failure of military professionalism.

Finally, let us return briefly to the question of military professionalism and ethics. In the bureaucratic world of the U.S. military today, ethics for all practical purposes amounts to little more than broad slogans—"honor, courage, commitment" in the case of the Navy and Marine Corps—supported by a labyrinth of quasi-legal programmatic regulations and mandatory training requirements. The focus is on preventing negative outcomes rather than encouraging positive ones, but the implicit message is one of lack of trust in the force to do the right thing. Any attempt to recover a genuine and robust professionalism in the Armed Forces should begin by coming to grips with this profoundly demoralizing state of affairs. JFQ

Notes

[1] The classic account is Thomas E. Ricks, *Making the Corps* (New York: Simon & Schuster, 1997).

[2] Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge, MA: Harvard University Press, 1957). See also Morris Janowitz,

General Dempsey testifies on sexual assault in military before U.S. Senate Arms Services Committee, June 2013 (DOD/Sean K. Harp)

The Professional Soldier: A Social and Political Portrait (New York: Free Press, 1960).

[3] Gayle L. Watkins and Randi C. Cohen, "In Their Own Words: Army Officers Discuss Their Profession," in The F*uture of the Army Profession* 2nd ed., dir. Don M. Snider and ed. Lloyd J. Matthews (Boston: McGraw Hill, 2005), chap. 5.

[4] Huntington, chap. 4.

[5] For a recent perspective, see especially Mackubin Thomas Owens, *U.S. Civil-Military Relations After 9/11: Renegotiating the Civil-Military Bargain* (London: Continuum, 2011).

[6] The contemporary debate on civilian control of the U.S. military was initiated by Richard H. Kohn, "Out of Control," *The National Interest* 35 (Spring 1994), 3–17. On the combatant commanders' role, see Dana Priest, *The Mission: Waging War and Keeping Peace with America's Military* (New York: Norton, 2003), as well as Carnes Lord, *Proconsuls: Delegated Political-Military Leadership from Rome to America Today* (Cambridge: Cambridge University Press, 2012), chap. 8.

[7] See James Burk, "Expertise, Jurisdiction, and Legitimacy of the Military Profession," in *The Future of the Army Profession*, chap. 2.

[8] Justin Kelly and Mike Brennan, *Alien: How Operational Art Devoured Strategy* (Carlisle Barracks, PA: U.S. Army War College, September 2009).

[9] See especially Richard Lacquement, "Mapping Army Professional Expertise and Clarifying Jurisdictions of Practice," in *The Future of the Army Profession*, chap. 9; and Nadia Schadlow, Charles Barry, and Richard Lacquement, "A Return to the Army's Roots: Governance, Stabilization, and Reconstruction," in *The Future of the Army Profession*, chap. 11.

[10] H.R. McMaster, *Dereliction of Duty: Lyndon Johnson, Robert McNamara, the Joint Chiefs of Staff, and the Lies That Led to Vietnam* (New York: HarperCollins, 1997).

President Obama speaks at DHS about how his budget would safeguard cyberspace and strengthen national preparedness and resilience (DHS/Jetta Disco)

Detangling the Web

A Screenshot of U.S. Government Cyber Activity

By G. Alexander Crowther and Shaheen Ghori

> *The world must collectively recognize the challenges posed by malevolent actors' entry into cyberspace, and update and strengthen our national and international policies accordingly. Activities undertaken in cyberspace have consequences for our lives in physical space, and we must work towards building the rule of law, to prevent the risks of logging on from outweighing its benefits.*
>
> —U.S. International Strategy for Cyberspace, May 2011

Blackouts. School testing. Electrical grids. Insurance. These all have one major thing in common: they have all been targets for cyber attacks in a period of two weeks during March 2015. The United States faces thousands of cyber assaults every day. States, state-sponsored organizations, other groups and individuals all combine to incessantly probe, spy on, and attack public and private organizations as well as denizens of the United States. These ongoing problems require a U.S. Government response, so it adopted a bureaucratic approach that

Dr. G. Alexander Crowther is Deputy Director of the Center for Technology and National Security Policy (CTNSP), Institute for National Strategic Studies, at the National Defense University. Shaheen Ghori has a Bachelor of Arts in International Relations from American University and is entering the Intelligence Community.

has resulted in a complex system that is constantly evolving as new problems are recognized. This article provides a comprehensive look at how the United States has organized to address these challenges. Although U.S. Government efforts seem sizable, private use of the Internet dwarfs government usage.[1]

Policies and Strategies

The U.S. Government articulates its cyber policy through a series of initiatives, policy decisions, and published strategies. The foundational document of the U.S. Government's approach to cyber policy is National Security Policy Decision 38, *The National Strategy to Secure Cyberspace*, dated July 7, 2004. Since its publication, a number of new policies and strategies have appeared that refine the government's approach. A short list includes:

- *Comprehensive National Cybersecurity Initiati*ve, March 2, 2010
- *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, July 6, 2010
- *International Strategy for Cyberspace*, May 2011
- Presidential Policy Directive (PPD) 20, *U.S. Cyber Operations Policy*, October 16, 2012
- National Cybersecurity Protection Act of 2014, December 18, 2014
- Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing,* February 13, 2015.

The capstone document is the 2015 *National Security Strategy*, which states:

Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution. Drawing on the voluntary cybersecurity framework, we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure.[2]

The President has further refined the document and identified his five priorities for cyber issues:[3]

- protecting the country's critical infrastructure—our most important information systems—from cyber threats
- improving the public- and private-sector abilities to identify and report cyber incidents to enable responses in a timely manner
- engaging with international partners to promote Internet freedom and build support for open, interoperable, secure, and reliable cyberspace
- securing Federal networks by setting clear security targets and holding agencies accountable for meeting targets
- shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.

Cyber Legislation

The Executive Branch's approach to the U.S. Government's cyber posture has yet to be mirrored in legislation affecting the private sector. There are four major problems. First is the sheer size and complexity of the U.S. infosphere, still the largest national component of the global system. The second involves conflicting political aims—the desire to provide effective information-sharing to identify potential threats versus the deeply ingrained national desire for personal privacy and suspicion of government overreach. The size and nature of the U.S. economy poses a third challenge. Private companies fear that information-sharing will lead to exposure to potential prosecution, the loss of proprietary information to competitors, and a loss of faith by their customers. A fourth challenge is the free-rider problem, with many participants in information-sharing schemes absorbing more information than they contribute, and with many participants treating information-sharing as marketing opportunities for their own security solutions.[4]

Legislation has fallen short for these reasons as well as the challenges of operating in a highly polarized partisan environment. The last major cyber legislation dates to 2002. Congress came close to passing comprehensive cyber security legislation in 2012 and 2013.[5] Efforts failed in 2012 because business balked at the prescriptive nature of proposed legislation, while the 2013 proposed legislation was overcome by political maneuvering leading up to the closing of the U.S. Government. Congress did pass the National Cybersecurity Protection Act,[6] Federal Information Security Modernization Act,[7] and Department of Homeland Security Cybersecurity Workforce Recruitment and Retention Act[8] in December 2014, which address various aspects of cyber security in the United States. Congress is currently working on comprehensive cyber legislation designed to address indemnity and liability with the goal of passing the legislation in the summer of 2015.

At the level of implementing the national-level policies and strategies, the boundaries between the various Federal agencies have also evolved. Today, the Department of Homeland Security (DHS), Department of Justice, and Department of Defense (DOD) share prominence but play discrete roles in countering the cyber threat.

Department of Homeland Security

DHS coordinates the national protection, prevention, and mitigation of and recovery from cyber incidents; disseminates domestic cyber threat and vulnerability analysis; protects critical infrastructure; secures Federal civilian systems (the dot.gov domain); and investigates cyber crimes under its jurisdiction.

The DHS vision is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards.[9] One of the five core missions of DHS is to safeguard and secure cyberspace, which involves the following components:

- strengthen the security and resilience of critical infrastructure
- secure the Federal civilian government information technology enterprise
- advance law enforcement, incident response, and reporting capabilities
- strengthen the (cyber) ecosystem.[10]

Subject matter expert assigned to Navy Information Assurance and Cyber Security Program Office demonstrates tactical key loader cryptographic key fill device (U.S. Navy/Rick Naystatt)

DHS essentially sees itself as facilitating the cyber neighborhood watch for the United States.[11] The core division of DHS that addresses cyber threats is the National Protection and Programs Directorate (NPPD), whose primary goal is to reduce the risks of homeland threats and make the physical and digital infrastructure of the U.S. Government more resilient and secure.[12] Within the NPPD, the most prominent cyber security offices are the Office of Cybersecurity and Communication (CS&C), Office of Infrastructure Protection, and Office of Cyber and Infrastructure Analysis. Outside of the NPPD, cyber security operations also take place within U.S. Immigrations and Custom Enforcement and the U.S. Secret Service.

CS&C works to prevent or minimize disruptions to critical information networks to protect the public, economy, and government services. It also leads efforts to protect the Federal dot.gov domain of civilian government networks and collaborate with the private sector—the dot.com domain—to increase the security of critical networks.[13] CS&C carries out its mission through its five divisions:

- The Office of Emergency Communications
- The National Cybersecurity and Communications Integration Center
- Stakeholder Engagement and Cyber Infrastructure Resilience
- Federal Network Resilience
- Network Security Deployment.

The CS&C Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division is the primary DHS point of engagement and coordination for national security/emergency preparedness (NS/EP) communications and cybersecurity initiatives for both government and industry partners, and is the Executive Secretariat for the Joint Program Office for the NS/EP Communications Executive Committee. CS&C relies on SECIR to streamline coordination and engagement with external partners, while leveraging capabilities and significant subject matter expertise to meet stakeholder requirements.[14]

The National Cybersecurity and Communications Integration Center (NCCIC) serves as a focal point for coordinating cyber security information-sharing with the private sector; provides technical assistance, onsite analysis, mitigation support, and assessment assistance to cyber attack victims, as well as situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure; and coordinates the national response to significant cyber incidents affecting critical infrastructure.[15] Under the National Infrastructure Protection Plan framework, the collaborative activity of the NCCIC blends together the interdependent missions of the National Coordinating Center for Telecommunications, U.S. Computer Emergency Readiness Team (US-CERT), DHS Office of Intelligence and Analysis, and National Cyber Security Center.[16] The NCCIC mission is to reduce the likelihood and severity of incidents against the Nation's critical technology and communications networks[17] and to build capacity and resilience in other organizations[18] through its four branches: the NCCIC Operations and Integration, US-CERT, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and National Coordination Center for Communications (NCC).

US-CERT provides a single accountable focal point to improve the Nation's cyber security posture, coordinate cyber information-sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans.[19] Additionally, US-CERT collaborates with Federal agencies; the private sector; the research community; academia; state, local, and tribal governments; and international partners. Through coordination with various national security incident centers in responding to potential security events and threats on both classified and unclassified networks, US-CERT disseminates cyber security information to the public.[20]

ICS-CERT operates cyber security operations centers that focus on responding to and analyzing control systems–related incidents; conducting vulnerability, malware, and digital media analysis; providing onsite incident response services; providing situational awareness in the form of actionable intelligence; coordinating the responsible disclosure of vulnerabilities and associated mitigations; and sharing and coordinating vulnerability information and threat analysis through information products and alerts.[21]

The NCC continuously monitors national and international incidents and events that may impact emergency communications. NCC works with both US-CERT and ICS-CERT to monitor and resolve issues impacting cyber and communications during an emergency.[22]

The Office of Infrastructure Protection leads the coordinated national effort to reduce risk to critical U.S. infrastructure and to help respond and quickly recover in case of terrorist attacks, natural disasters, or other emergencies. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators, as well as state, local, tribal, and territorial partners understand and address risks.[23] The office is the sector-specific agency for six of the critical infrastructure sectors: chemical, commercial facilities, critical manufacturing, dams, emergency services, and nuclear,

The Office of Cyber and Infrastructure Analysis implements PPD 21, which calls for integrated analysis of critical infrastructure, and Executive Order 13636, which identifies critical infrastructure where cyber incidents could have catastrophic impacts to public health and safety, the economy, and national security. The mission is to support efforts to protect the Nation's critical infrastructure by providing analytic support to DHS leadership, operational components, and field personnel during steady-state operations and crises on emerging threats and incidents; assessing and informing national risk management strategies on the likelihood and consequence of emerging and future risks; and developing and enhancing capabilities to support crisis actions by identifying and prioritizing infrastructure through the use of analytic tools and modeling capabilities.[24]

Homeland Security Investigations (HSI) operates the Cyber Crime Center (C3), which is responsible for providing domestic and international training and the support, coordination, and deconfliction of cyber investigations related to online economic crime, digital theft of export-controlled data, digital theft of intellectual property, and online child exploitation investigations. This state-of-the-art center offers cyber crime support and training to Federal, state, local, and international law enforcement agencies.[25] The most important sector of the C3 in dealing with cyber security is the Cyber Crimes Unit, which provides the management and oversight of the agency's cyber-related investigations by focusing on the transnational criminal organizations that use cyber capabilities to further their capital enterprise. This unit provides training, investigative support, and guidance to HSI field offices in emerging cyber technologies as well as subject matter expertise in cyber-related investigations related to identity and benefit document fraud, money-laundering, financial fraud, commercial fraud, counterproliferation investigations, narcotics-trafficking, and illegal exports.[26]

The Secret Service leads a network of electronic crimes task forces to bring together Federal, state, and local law enforcement, prosecutors, private industry, and academia for the common purpose of preventing, detecting, mitigating, and investigating various forms of malicious cyber activity. The Secret Service also runs the National Computer Forensics Institute, a training center dedicated to providing state and local law enforcement and legal and judicial professionals a free, comprehensive education on current cyber crime trends, investigative, methods, and prosecutorial and judicial challenges.[27]

Department of Justice

The Department of Justice investigates, attributes, disrupts, and prosecutes cyber crimes; has the lead for domestic national security operations; conducts domestic collection, analysis, and dissemination of cyber threat intelligence; supports the national protection, prevention, mitigation of, and recovery from cyber incidents; and coordinates cyber threat investigations.

Justice developed its 2014–2018 strategy to include priorities and programs that address the President's priorities.[28] Its number one goal is to "prevent terrorism and promote the nation's security consistent with the rule of law," and it aligns cyber efforts under that goal. It intends to combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors.[29] Its cyber strategy involves an all-tools approach including both investigation and prosecution, with a focus on the disruption of the threat.[30]

The Federal Bureau of investigation (FBI) leads the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud by gathering and sharing information and intelligence with public- and private-sector partners worldwide.[31] It has developed a number of initiatives to perform these missions. Internally, the headquarters now contains the Cyber Division to bring together various FBI cyber initiatives and missions and has placed cyber task forces in all 56 field offices to focus exclusively on cyber security threats and synchronize domestic cyber threat investigations in the local community.[32]

The Cyber Action Team (CAT) is the FBI Cyber Division's investigative rapid response team that can be on scene within 48 hours. The CAT mission is to deploy globally at the direction of FBI Cyber Division to bring in-depth cyber intrusion expertise and specialized investigative skills to initiatives, cases, and emergencies deemed critical and significant. When deployed, CAT objectives are to provide support to the local field office to make the case move as quickly and effectively as possible and to provide detailed intrusion analysis using a blend of FBI investigative techniques.

Today, the National Cyber Investigative Joint Task Force (NCIJTF) is the focal point for government agencies to coordinate, integrate, and share information related to domestic cyber threat investigations. The FBI is the executive agent for the joint task force and partners with the National Security Agency (NSA), Central Intelligence Agency, Secret Service, DHS, and United States Cyber Command (USCYBERCOM). Its five mission areas include coordinating whole-of-government campaigns against known cyber threats, exploiting valuable cyber data, analyzing and reporting on that data, applying traditional financial investigative approaches to the cyber domain, and maintaining an around-the-clock cyber incident management watch. Because task force members represent many state, Federal, and international jurisdictions, collaboration at the NCIJTF is critical to ensuring that all legal means and resources available are used to track, attribute, and take action against these cyber threats and to ultimately place international cyber criminals behind bars and off our global networks.

Other examples of cyber collaboration fostered by the FBI are:

- InfraGard, an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.
- The National Cyber-Forensics and Training Alliance, which has become an international model for bringing together law enforcement, private industry, and academia to share information to stop emerging cyber threats and mitigate existing ones.[33]
- The Strategic Alliance Cyber Crime Working Group, started at FBI headquarters in September 2006, which consists of cyber law enforcement bodies from Australia, Canada, New Zealand, the United Kingdom, and the United States.[34]

The Justice Department's National Security Division and Criminal Division each concentrates on its own cyber issues. The division deals with cyber-based threats to the national security.[35] It created the National Security Cyber Specialist network that is a new tool in the government's cyber toolkit and a critical part of the department's efforts to better address cyber intrusions and attacks carried out by nation-states or terrorist organizations.[36]

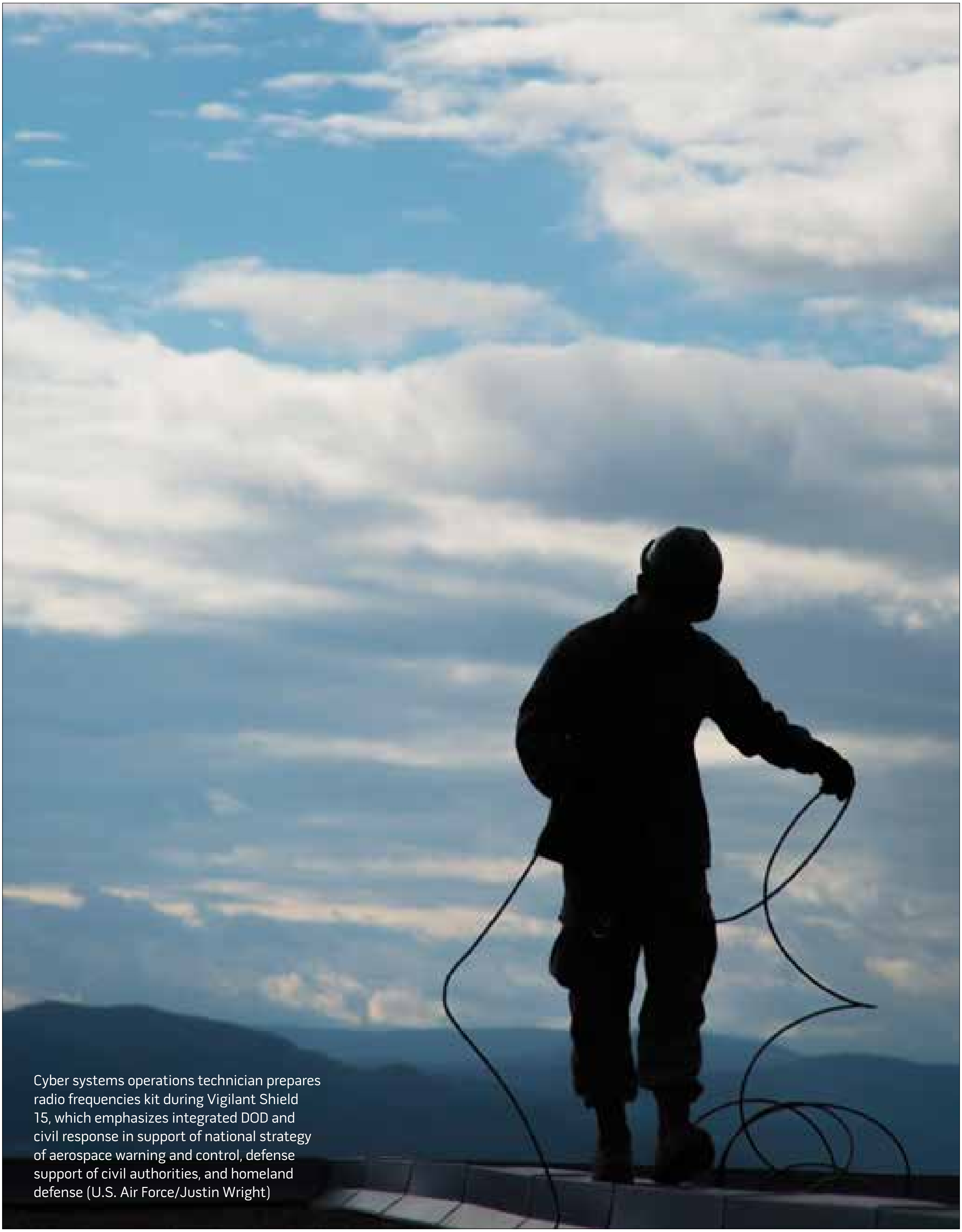
The Criminal Division contains the Computer Crime and Intellectual Property Section (CCIPS), which implements Justice's national strategies in combating computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. In pursuing all these goals, CCIPS attorneys regularly run complex investigations; resolve unique legal and investigative issues raised by emerging computer and telecommunications technologies; litigate cases; provide litigation support to other prosecutors; train Federal, state, and local law enforcement personnel; comment on and propose legislation; and initiate and participate in international efforts to combat computer and intellectual property crime.[37]

The Offices of the U.S. Attorneys is the last major part of Justice that works cyber issues. One of their 10 priority areas is cyber crime.[38] Their three areas of concentration are Internet stalking, computer hacking, intellectual property rights and forensics. They also assist the National Computer Forensics Institute.

Department of Defense

The DOD mission is to secure the Nation's freedom of action in cyberspace and help mitigate risks to national security resulting from America's growing dependence on cyberspace. Specific mission sets include directing, securing, and defending DOD Information Network (DODIN) operations (including the dot.mil domain); maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; and providing support to civil authorities and international partners.[39]

DOD articulates its cyber policy through the *DOD Strategy for Operating in Cyberspace*, dated July 2011, and Joint Publication 3-12, *Cyberspace Operations*, dated February 5, 2013. DOD's operations are designed to achieve and maintain *cyberspace superiority*, defined as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary."[40] DOD organizations are allowed



Cyber systems operations technician prepares radio frequencies kit during Vigilant Shield 15, which emphasizes integrated DOD and civil response in support of national strategy of aerospace warning and control, defense support of civil authorities, and homeland defense (U.S. Air Force/Justin Wright) to perform defensive cyber operations; however, full-spectrum cyber operations (including offensive cyber operations) are approved by the President and directed by the Secretary of Defense.[41]

Combatant Commands (CCMDs) provide operations instructions and command and control to the Armed Forces and have a significant impact on how they are organized, trained, and resourced—areas over which Congress has constitutional authority.[42] CCMDs share cyber information largely through USCYBERCOM and their own joint cyber centers, but various personnel also meet periodically to share information in collaboration sessions.[43]

The National Security Agency is the Nation's cryptologic organization that coordinates, directs, and performs highly specialized activities to protect U.S. information systems and to produce foreign signals intelligence information. It supports military customers, national policymakers, and the counterterrorism and counterintelligence communities, as well as key international allies. The NSA also shares information about software vulnerabilities with vendors and users in any commercial product or system (not just software) used by the United States and its allies, with an emphasis on risk mitigation and defense.[44]

The Defense Information Systems Agency (DISA) provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations. They are overall responsible for DODIN. Each Service also has its own equivalent to DISA that operates its part of DODIN.

The Defense Cyber Crime Center delivers superior digital forensics and multimedia laboratory services, cyber technical training, research, development, testing and evaluation, and cyber analysis capabilities supporting cyber counterintelligence and counterterrorism, criminal investigations, intrusion forensics, law enforcement, the Intelligence Community, critical infrastructure partners, and information operations for DOD.[45]

USCYBERCOM was formed in 2010 by consolidating two U.S. Strategic Command (USSTRATCOM) subordinate organizations: the Joint Functional Component Command–Network Warfare and Joint Task Force–Global Network Operations.[46] It is a subunified command under USSTRATCOM. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified DODIN. It also prepares, when directed, to conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure U.S./allied freedom of action in cyberspace and deny the same to adversaries.[47]

USCYBERCOM's main instrument of power consists of the Cyber National Mission Force, which conducts cyberspace operations to disrupt and deny adversary attacks against national critical infrastructure. It is the U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations. It plans to create 133 cyber mission teams by the end of fiscal year 2016, which will consist of National Mission Teams, which perform full-spectrum cyber operations; National Support Teams, which provide direct support to the National Missions Teams; and National Cyber Protection Teams, which protect whomever they are assigned to.

Combat Mission Forces are similar to the National Mission Teams but rather than serving at the national level, they conduct cyberspace operations to achieve combatant commanders' objectives and are geographically and functionally aligned under one of four Joint Force Headquarters–Cyber (JFHQ-C) in direct support of geographic and functional CCMDs:

- JFHQ-C Washington supports U.S. Special Operations Command, U.S. Pacific Command, and U.S. Southern Command.
- JFHQ-C Georgia supports U.S. Central Command, U.S. Africa Command, and U.S. Northern Command.
- JFHQ-C Texas supports U.S. European Command, USSTRATCOM, and U.S. Transportation Command.[48]
- JFHQ-DODIN defends DOD information networks at USCYBERCOM.[49]

The Services and Cyber. The Service chiefs will provide cyber operations capabilities for deployment/support to CCMDs as directed by the Secretary of Defense and remain responsible for compliance with USSTRATCOM's direction for operation and defense of the DODIN.[50] In addition to the joint strategy and doctrine, each Service also has its own doctrine to deal with cyber issues:

- The Army publishes Field Manual 3-38, *Cyber Electromagnetic Activities*, and is currently developing a new Cyber Branch and Military Occupational Specialty to facilitate the development of its cyber workforce.
- The Navy has a set of approaches including the *Department of the Navy Cybersecurity/Information Assurance Workforce Management, Oversight and Compliance*; the *Navy Information Dominance Corps Human Capital Strategy 2012–2017*; *Navy Cyber Power 2020*; the *U.S. Navy Information Dominance Roadmap 2013–2028*; and the *Navy Strategy for Achieving Information Dominance 2013–2017*. The Service created the Information Dominance Corps, a unified body that produces precise, timely warfighting decisions[51] by bringing together the intelligence, information professional, information warfare, meteorology and oceanography communities, and members of the space cadre.
- The Marine Corps has Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations*. The Service recognizes five types of cyber operations: network operations, defensive and offensive cyber operations, computer network exploitation, and information assurance.
- The Air Force codified its cyber doctrine in Air Force Doctrine Document 3-12, *Cyberspace Operations*, published in 2010 and updated in 2011.[52]

It has also created its own cyber branch by carving out part of the Air Force communications community.

Each of the Services also has its own cyber organizations. Under their Title 10 role as force providers to the combatant commanders, the Services recruit, train, educate, and retain the military cyber force. These are U.S. Army Cyber Command/2nd U.S. Army, U.S. Fleet Cyber Command/U.S. 10th Fleet, 24th Air Force, and U.S. Marine Corps Forces Cyber Command.[53]

Service-Specific Structure. U.S. Army Cyber Command or 2nd U.S. Army is the single information technology provider for all network communications and is responsible for the Army section of the DODIN.[54] The U.S. Intelligence and Security Command conducts intelligence, security, and information operations for military commanders and national decisionmakers.[55] The command is also responsible for the Joint Forces Headquarters Cyber in Georgia.

U.S. Fleet Cyber Command (FCC) and 10th Fleet compose combined headquarters at Fort Meade, Maryland. FCC is the staff organization to organize forces, and 10th Fleet is the operational staff that provides command and control.[56] FCC has a mission set similar to the other Services: direct cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; organize and direct cryptologic operations worldwide and support information operations and space planning and operations, as directed; execute cyber missions as directed; direct, operate, maintain, secure, and defend the Navy's portion of the DODIN; deliver integrated cyber, information operations, cryptologic, and space capabilities; deliver global cyber network operational requirements; assess cyber readiness; and manage, man, train, and equip functions associated with Navy Component Commander and Service Cryptologic Commander responsibilities.[57] The mission of 10th Fleet is to serve as the Numbered Fleet for Fleet Cyber Command and exercise operational control of assigned forces and to coordinate with other naval, coalition, and joint task forces to execute the full spectrum of cyber, electronic warfare, information operations, and signal intelligence capabilities and missions across the cyber, electromagnetic, and space domains.[58]

Marine Corps Forces Cyber Command has two subordinate elements: the Marine Corps Network Operations and Security Center and L Company of the Marine Corps Support Battalion.[59] It has also been innovative in its deployment of cyber forces, with the Marine Air-Ground Task Force Cyberspace and Electronic Warfare Coordination Cell being embedded into the Marine Expeditionary Unit onboard ships where it provides support directly to deployed forces.

Air Forces Cyber or the 24th Air Force is self-described as an "Operational war-fighting organization that executes full spectrum cyberspace operations to ensure friendly forces maintain a warfighting advantage."[60] It has several subordinate elements:

- 624th Operations Center serves as the cyber operations center for the Air Force.
- 67th Cyberspace Wing operates the Air Force Information Network, which is the Air Force section of DODIN.
- 688th Cyberspace Wing delivers proven information operations engineering and infrastructure capabilities.
- 5th Combat Communications Group delivers expeditionary communications, information systems, engineering and installation, air traffic control, and weather services to the President, Secretary of Defense, and combatant commanders.[61]

Conclusion

The United States both benefits from and is challenged by a wide variety of Federal Government actors in the cyber realm. The benefit comes from pursuing multiple responses simultaneously, leading to agility and greater defense in-depth. However, this same approach is far more expensive and may lead to confusion with private-sector stakeholders and an increased level of competition for limited skilled resources. The abundance of Federal Government actors was not a planned response. Many of these organizations were created as the result of bottom-up initiatives from within the various departments seeking to respond to an emerging, ill-defined threat area. Executive branch decision memoranda, policy statements, and strategies are beginning to bring some organization to the interdepartmental effort; however, a statutory blueprint (with corresponding budgetary guidance) has yet to be approved by Congress. Whether it is wise to prune the Federal Government's response to the cyber threat is a policy decision yet to be made, but the current state of affairs clearly requires a map to understand its full scale and scope. This article has looked at the structure that exists in 2015. No doubt the structure, roles, and missions will continue to change as the cyber realm itself matures. JFQ

Notes

[1] Interview with Brigadier General Greg Touhill, USAF (Ret.), Deputy Assistant Secretary of Homeland Security, Cyber Security Operations Program, March 27, 2015.

[2] *National Security Strategy* (Washington, DC: The White House, February 2015), 12–13, available at <www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.

[3] "Cybersecurity," The White House, March 18, 2015, available at <www.whitehouse.gov/issues/foreign-policy/cybersecurity>.

[4] Testimony of Steven R. Chabinsky before the U.S. Senate Committee on Homeland Security and Governmental Affairs, "Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure," Washington, DC, March 26, 2014.

[5] The authors would like to thank Thomas Wingfield, Esq., for providing his thoughts on cyber legislation.

[6] "S.2519—National Cybersecurity Protection Act of 2014," U.S. Congress, December, 18, 2014, available at <www.congress.gov/113/bills/s2519/BILLS-113s2519enr.pdf>.

[7] "S.2521—Federal Information Security Modernization Act of 2014," U.S. Congress, December 18, 2014, available at <www.congress.gov/113/bills/s2521/BILLS-

113s2521enr.pdf>.

[8] "S.2354—DHS Cybersecurity Workforce and Recruitment and Retention Act of 2014," U.S. Congress, July 14, 2014, available at <www.congress.gov/113/bills/s2354/BILLS-113s2354rs.pdf>.

[9] "Our Mission," Department of Homeland Security (DHS), available at <www.dhs.gov/our-mission>.

[10] "The 2014 Quadrennial Homeland Security Review," DHS, June 18, 2014, 78, available at <www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>.

[11] Touhill interview.

[12] Touhill interview; and "NPPD at a Glance," DHS, available at <www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf>.

[13] Touhill interview; and "Office of Cybersecurity and Communications," DHS, available at <www.dhs.gov/office-cybersecurity-and-communications>.

[14] "Stakeholder Engagement and Cyber Infrastructure Resilience," DHS, available at <www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience>.

[15] "The 2014 Quadrennial Homeland Security Review."

[16] "Cybersecurity: DHS's Role, Federal Efforts, and National Policy," U.S. Government Printing Office (GPO), June 16, 2010, 12, available at <www.gpo.gov/fdsys/pkg/CHRG-111hhrg64697/pdf/CHRG-111hhrg64697.pdf>.

[17] "National Cybersecurity Communications Integration Center," DHS, available at <www.dhs.gov/about-national-cybersecurity-communications-integration-center>.

[18] Touhill interview.

[19] "About Us," U.S. Computer Emergency Response Team, available at <www.us-cert.gov/about-us>.

[20] "Cybersecurity: DHS's Role, Federal Efforts, and National Policy," GPO, June 16, 2010, 15, available at <www.gpo.gov/fdsys/pkg/CHRG-111hhrg64697/pdf/CHRG-111hhrg64697.pdf>.

[21] "About the Industrial Control Systems Cyber Emergency Response Team," Industrial Control Systems Cyber Emergency Response Team, available at <https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team>.

[22] "National Coordinating Center for Communications," DHS, available at <www.dhs.gov/national-coordinating-center-communications#>.

[23] "Office of Infrastructure Protection Strategic Plan: 2012–2016," DHS, available at <www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf>.

[24] "Office of Cyber and Infrastructure Analysis," DHS, available at <www.dhs.gov/office-cyber-infrastructure-analysis>.

[25] "Cyber Crimes Center," U.S. Immigration and Customs Enforcement, available at <www.ice.gov/cyber-crimes>.

[26] Ibid.

[27] "About," National Computer Forensics Institute, available at <www.ncfi.usss.gov/ncfi/pages/about.jsf>.

[28] "Strategic Plan Fiscal Years 2014–2018," U.S. Department of Justice (DOJ), available at <www.justice.gov/about/strategic-plan-fiscal-years-2014-2018>.

[29] Ibid., 10.

[30] Ibid., 19.

[31] "Cyber Crime," Federal Bureau of Investigation (FBI), available at <www.fbi.gov/about-us/investigate/cyber>.

[32] "Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity," FBI, available at <www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1>.

[33] "The NCFTA: Combating Force to Fight Cyber Crime," FBI, September 16, 2011, available at <www.fbi.gov/news/stories/2011/september/cyber_091611>.

[34] "Cyber Solidarity: Five Nations, One Mission," FBI, March 18, 2008, available at <www.fbi.gov/news/stories/2008/march/cybergroup_031708>.

[35] "Combatting National Security Cyber Threats," DOJ, available at <www.justice.gov/nsd/about-division-0>.

[36] "New Network Takes Aim at Cyber Threats to National Security," DOJ, November 14, 2012, available at <www.justice.gov/opa/blog/new-network-takes-aim-cyber-threats-national-security>.

[37] "Computer Crime and Intellectual Property Section," DOJ, available at <www.justice.gov/criminal/cybercrime/>.

[38] "Cyber Crime," Offices of the U.S. Attorneys, available at <www.justice.gov/usao/priority-areas/cyber-crime>.

[39] Vice Admiral Michael S. Rogers, USN, Nominee for Commander, U.S. Cyber Command, Congressional Testimony, March 11, 2014.

[40] Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, February 5, 2013), GL-4, available at <www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>.

[41] Rogers Congressional Testimony, March 11, 2014.

[42] Andrew Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," R42077 (Washington, DC: Congressional Research Service, January 3, 2013), available at <http://fas.org/sgp/crs/natsec/R42077.pdf>.

[43] Rita Boland, "Command's Cybersecurity Crosses Domains, Directorates," *Signal*, June 1, 2013, available at <www.afcea.org/content/?q=command%E2%80%99s-cybersecurity%E2%80%A8-crosses-domains-directorates>.

[44] Rogers Congressional Testimony, March 11, 2014.

[45] "Mission," Defense Cyber Crime Center, available at <www.dc3.mil/index/mission>.

[46] U.S. Cyber Command's Web site is available at <www.jtfgno.mil>.

[47] "Mission Statement," U.S. Cyber Command, available at <www.jtfgno.mil/default.aspx>.

[48] "Advance Questions for Vice Admiral Michael S. Rogers," Senate Armed Services Committee, March 11, 2014, available at <http://fas.org:8080/irp/congress/2014_hr/031114rogers-q.pdf>.

[49] "Statement of Admiral Michael S. Rogers," Senate Armed Services Committee, March 19, 2015, available at <http://fas.org:8080/irp/congress/2015_hr/031915rogers.pdf>.

[50] JP 3-12(R), ix.

[51] "Navy Information Dominance Corps Human Capital Strategy 2012–2017," U.S. Navy, iv, available at <www.public.navy.mil/fcc-c10f/Strategies/Navy_Information_Dominance_Corps_Human_Capital_Strategy.pdf>.

[52] Air Force Doctrine Document 3-12, *Cyberspace Operations*, U.S. Air Force, July 15, 2010 (updated November 30, 2011).

[53] "DOD Strategy for Operating in Cyberspace," DOD, July 2011, available at <www.defense.gov/news/d20110714cyber.pdf>.

[54] "NETCOM," U.S. Army Cyber Command, available at <www.arcyber.army.mil/org-netcom.html>; and <www.army.mil/info/organization/unitsandcommands/command-structure/netcom/>.

[55] "INSCOM," U.S. Army Cyber Command, available at <www.arcyber.army.mil/org-inscom.html>; and <www.inscom.army.mil/>.

[56] Email from CAPT Stephanie Keck, Division Director, Information Dominance Corps and Foreign Area Officer Assignments, Navy Personnel Command.

[57] "U.S. Fleet Cyber Command Mission and Vision," U.S. Fleet Cyber Command, available at <www.fcc.navy.mil/>.

[58] "U.S. Tenth Fleet Mission," U.S. Fleet Cyber Command, available at <www.fcc.navy.mil/>.

[59] Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations* (Washington, DC: Department of the Navy, Headquarters U.S. Marine Corps, August 9, 2011), 2-17 and 2-18.

[60] "24th Air Force Fact Sheet," *24th Air Force*, available at <http://newpreview.afnews.af.mil/24af/library/factsheets/factsheet.asp?id=15663>.

[61] "24th Air Force Units," *24th Air Force*, available at <www.24af.af.mil/units/index.asp>.

Dr. Josh Kvavle, right, demonstrates Google Glass headset for Chief of Naval Operations Admiral Jonathan Greenert during Rapid Innovation Cell meeting (U.S. Navy/Peter D. Lawlor)

One Size Does Not Fit All
The Multifaceted Nature of Cyber Statecraft

By Andrea Little Limbago

Cyberspace is frequently referred to as the fifth domain, alluding to its perceived role as the next major battlefield after land, sea, air, and space. However, this oversimplification of cyberspace underestimates its transformational impact within and across each of these domains. Moreover, framing cyber solely as a battlefield and coercive domain ignores the diverse ways in which both state and nonstate actors use cyber statecraft to pursue their objectives. It is an understatement to say that the introduction of cyberspace as a fifth domain has had disruptive effects on the international system, but to date there has been little discussion on the myriad ways in which actors exploit cyberspace for geopolitical gain. From Stuxnet at one extreme to government-sponsored Facebook accounts at the other, digital disruption has significantly increased the tools available to state and nonstate actors. Even transitions of power are now often first publicized in cyberspace. For example, following the recent coup in Thailand, martial law was officially declared via Twitter and a new Facebook account and was dubbed by some researchers as a *#cybercoup*.

To better evaluate the strategic implications of cyber as a domain in which to achieve national security objectives—from antiaccess/area denial to governance, democratization, and economic growth—policymakers need a rigorous, multifaceted framework that examines cyber statecraft not only as a military tool, but also as a more holistic form of statecraft. Such a framework is long overdue to help make sense of the great technological disruption that continues to shape the international political system. While the military component is essential, cyber statecraft is often viewed

Dr. Andrea Little Limbago is the Principal Social Scientist at Endgame, a security intelligence and analytics software company.

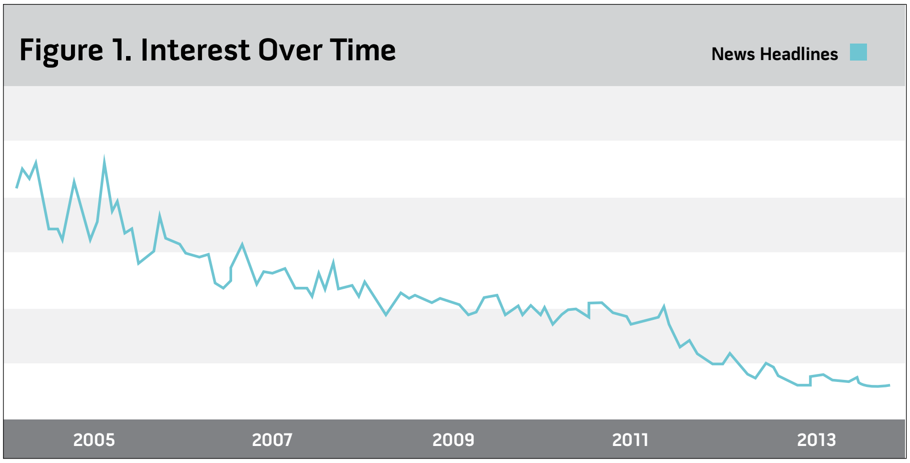


Figure 1. Interest Over Time

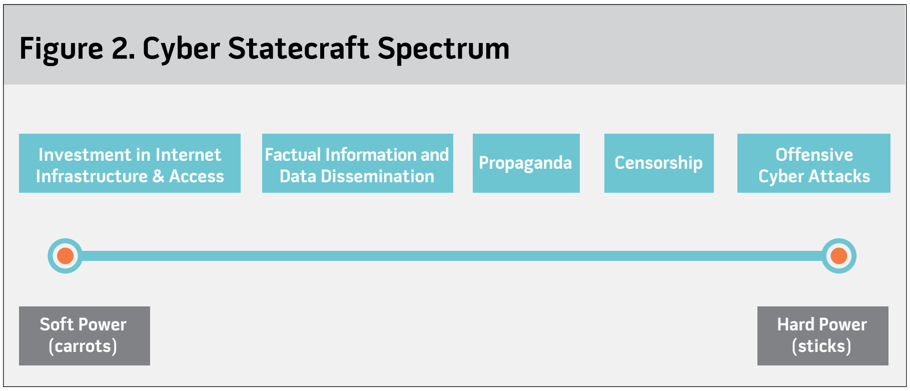


Figure 2. Cyber Statecraft Spectrum

Investment in Internet Infrastructure & Access
Factual Information and Data Dissemination
Propaganda
Censorship
Offensive Cyber Attacks
Soft Power (carrots)
Hard Power (sticks)

only through this coercive lens, when in fact it is much broader. Even within the military aspects of cyber statecraft, little has been written about the various tools available to actors in this domain, which has led to everything from cyber censorship to cyber espionage being lumped together under the broad umbrella of *cyber attacks*. These comparisons greatly impede the ability of practitioners and theorists alike to assess the strategic implications of cyber statecraft.

In comparing cyber studies to the evolution of nuclear strategic studies, Joseph Nye notes, "Strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950."[1] In short, cyberspace analyses and theories lag behind changes in the operating environment, resulting in a theoretical and operational void that has strategic implications. The classification of cyberspace as solely a domain of conflict has contributed to this theoretical stagnation, limiting policymakers' understanding of the ways in which cyberspace can be leveraged for broader applications of statecraft. But the militarization of cyberspace is not the only culprit here; the gap between the technical and national security policy communities is also partially to blame. The technical nature of discussions on cyberspace has hindered a coherent understanding of cyber as statecraft. Moreover, the phenomenal speed of technological change has rendered it difficult for policymakers and the larger strategic studies community to remain apace of developments within the cyber domain.

The Cyber Statecraft Spectrum

On the surface, it may seem pedantic to build a theoretical framework for analyzing and understanding the various implementations of cyber statecraft. Lacking such a framework, however, cyber statecraft risks perpetuating the perception that it is solely an offensive tool. In his book *A Fierce Domain*, Jason Healey notes the increasing militarization of the term *cyber*.[2] While initially a neutral term, current references to cyber generally imply offensive behavior, while *Internet* is used when discussing the positive technological impacts of cyberspace. In fact, discussion of cyberspace as a unique domain has decreased dramatically over the last 15 years. This trend is quite stark when conducting a quick review of Google search term trends for *cyberspace*, as depicted in figure 1. Cyber is increasingly used as a prefix for a variety of offensive activities such as cyberwar, cybercrime, and cyber attacks.

This trend parallels changes in perceptions of economic statecraft, which was initially viewed as a form of state coercive power. As mercantilism gave way to a more liberal global economy, strategists began to attribute pacifying effects to economic statecraft as well. The recognition of the potential of economic tools to promote peace and development helped ensure that economic statecraft was viewed as more than just a coercive tool in power politics. Just as economic statecraft generally refers to the use of economics as a persuasive political instrument, cyber statecraft can be similarly regarded as the use of cyber tools to achieve political objectives. Moreover, unlike other tools of statecraft, cyber tools are not pigeonholed into a discrete category. Cyber statecraft permeates each of the diplomatic, information, military, and economic elements of power. This likely is due to the unique nature of cyberspace and its multiple layers, including both the physical and communication domains. In each case, however, cyber statecraft serves as the means to achieve political goals within that element of power. Similar to the rise of economic statecraft during the mercantilist period, cyber statecraft has emerged as an omnipresent tool of choice in the current era of globalization and pervasive information technology.

Contrary to common perceptions, cyber statecraft is used to exert both hard power (that is, coercion, punishment) and soft power (such as persuasion to adopt

Maryam Mirzakhani was awarded 2014 Fields Medal—International Congress of Mathematicians' first female prize winner in its 80-year history—for "her outstanding contributions to the dynamics and geometry of Riemann surfaces and their moduli spaces" (courtesy of Maryam Mirzakhani)

similar goals, attraction), and everything in between. While by no means an exhaustive list, figure 2 depicts a broad categorization of the cyber tools most frequently employed, ranging from positive incentives for Internet freedom and access on one extreme to offensive cyber attacks on the other. This framework depicts the *physical* layers of cyberspace on either extreme of the spectrum, with the *communication* aspects occupying the middle ground.

The remainder of this article provides current, concrete examples of the use of cyber statecraft across the power spectrum and, in doing so, suggests a strategic framework for understanding and leveraging cyber as tool of statecraft. As the following examples illustrate, state and nonstate actors employ cyber statecraft in diverse ways to pursue a range of objectives. As with other forms of statecraft, cyber statecraft can be used for benign or malicious intents. In conjunction with the tool employed, intent becomes an additional determining factor of whether the application of cyber statecraft is a carrot or a stick. Therefore, the goal is not to provide an exhaustive overview of every tool possible within cyber statecraft, but rather to expand perceptions of cyberspace to include the diversity of tools accessible within this domain along the power spectrum. Moreover, as the examples illustrate, cyber statecraft is unique in its asymmetric nature, capable of empowering not only major powers but also serving as a means for weaker actors to have a disproportionate impact in the international arena.

Investment in Internet Infrastructure and Access

State investment in cyber infrastructure—while also promoting connectivity through physical infrastructure—fosters technology-driven solutions to a wide range of economic, political, and social issues that plague the developed and developing world alike. Many governments—and even some nonstate actors—implement cyber infrastructure to empower populations through the positive externalities that often coincide with Internet access. Therefore, government investment both in the expansion of physical infrastructure as well as in access to the Internet is absolutely essential for achieving political objectives. Information technology infrastructure—including the hardware as well as its legal aspects—serves as the mechanism through which governments transmit content used for attraction and persuasion. Numerous positive political and economic externalities have been associated with greater Internet access, especially in the developing world. Greater Internet access can increase private-sector competitiveness, enhance educational opportunities, and spark economic efficiencies. For instance, technological participation—only possible via an existing cyber infrastructure—can provide a means for reaching at-risk populations. Connectivity could become a key tool in combating radicalization by providing greater access to information, education, and economic opportunities as well as entertainment. The possible economic benefits are particularly prevalent in populations that rely on mobile money transfers and Internet banking as core components of their economy.

The potential for this soft power mode of cyber statecraft to shape the current geopolitical environment is likely to grow as Internet access continues to spread globally—especially as countries leapfrog archaic technologies in favor of modern communication systems. For instance, the 2012 World Bank report *Information and Communication for Development* identifies mobile broadband as having an even stronger impact on economic growth than fixed broadband.[3] In many developing countries, mobile money platforms enable both aid organizations and the domestic population to circumvent economic blockades and provide assistance as well as integration with the global economy.

Kenya is one of a growing number of countries that has received accolades for its concerted expansion of Internet access over the past few years. According to the World Bank World Development Indicators, Internet usage in Kenya has increased by 400 percent over the last 5 years.[4] This is significant, particularly since Kenya was threatened with rising unrest following a controversial election in 2007, when less than 10 percent of the population had Internet access. The impact of this expanded access is not solely economic. It also encourages the development of human capital through access to online education tools and information such as daily market prices—essential knowledge in agrarian areas. As Kenya's situation demonstrates, investments in Internet expansion are critical to a government's ability to provide the environmental conditions for the effective use of soft power. While not necessarily new, this phenomenon has recently received more rigorous attention as governments devote resources specifically for the creation and expansion of Internet architecture and a technology-based economy. In the 1970s, for example, India set aside an area near Bangalore to create an electronic city. However, the legal and economic systems lagged behind, and the information technology hub did not truly begin to emerge until economic liberalization took hold in the 1990s.

Building up a cyber architecture is not solely a tool for achieving inward-facing domestic objectives, but it is also emerging as a component of power politics as states vie for regional influence. For example, fiber networks and cell towers can be used to help build alliances between countries and expand a major power's sphere of influence. This tactic is also increasingly employed by some multinational corporations to achieve their own objectives. Google's Project Link, which aims to build fiber networks in Africa, is a case in point. Conversely, the Europe/Brazil effort to build an underwater cable with the goal of circumventing U.S. surveillance efforts demonstrates the role of power politics within cyberspace. Finally, the creation of cyber infrastructure could become a tool in peacekeeping missions and conflict interventions. Following a conflict, restoring the cyber infrastructure may become just as important as providing access to essential services such as security, water, and electricity as technology becomes the medium through which disparate aid efforts and financial assistance can be coordinated and systematically dispersed, while also serving as the bedrock for reconstructing postconflict political, economic, and social institutions.

Factual Information and Data Dissemination

While the popular discussion focuses heavily on Internet censorship, many state and nonstate actors also leverage cyberspace as a means to diffuse factual information to their populations, provide greater transparency, and signal their intent. In Iran, President Hassan Rouhani ran on a platform of greater Internet openness. While he has undoubtedly implemented coercive cyber tools, which will be discussed subsequently, Rouhani simultaneously uses his Twitter account to spread a more positive message of transparency. Recently, he used Twitter to congratulate Iranian mathematician and Fields Medal–winner Maryam Mirzakhani, and included a picture of her without a headscarf—an apparent attempt at demonstrating openness and preventing further "brain drain" from Iran. This is not a single occurrence with Rouhani. He also previously tweeted the content of his call with President Barack Obama following the September 2013 United Nations General Assembly in New York. Similarly, the Thai government's tweet announcing martial law can be viewed as a means of promoting transparency by openly disseminating critical information to the greater population. Twitter remains a mechanism through which the Thai people interact with the new military-led government.

Governments also employ cyber tools to defend their actions or indirectly signal intent that would be politically imprudent to express directly. For instance, President Dilma Rousseff used her Twitter account to defend Brazil's preparation for the World Cup. Prime Minister Shinzo Abe also appears to be using his Twitter account to signal to the Japanese people his foreign policy intentions. Abe only follows a handful of people on Twitter, but India's Prime Minister Narendra Modi is one of them. It is too soon to tell whether this indicates closer future ties between the two countries, but social media is an easy and subtle way to inform the population of a leader's intent or interests.

Finally, mobile technologies have provided the technological foundation for community policing programs in both the developing and the developed world. Rwanda has implemented crowd-sourcing initiatives that leverage mobile platforms to strengthen the rule of law, thereby enabling the community to pass along information regarding looting and violent incidents and to simply serve as citizen journalists. The crowd-sourcing of information for the purpose of depicting

Ohio National Guard Computer Network Defense Team members conduct operations during Cyber Shield 2015, March 2015, at Camp Atterbury, IN (Ohio National Guard/George Davis)

Slovenian soldier assesses mission group's response to cyber attack during Combined Endeavor 14, world's largest C4 systems exercise (U.S. Marine Corps Forces Europe/Derrick K. Irions) events factually and in real time is not limited to state actors but is actually a tactic employed more often by nonstate actors such as nongovernmental organizations as well as the general population. This is apparent during events as diverse as the Venezuelan protests, the Wenzhou train crash in China, and the recent Ebola crisis in West Africa. Of course, intent plays a key role in categorizing cyber behavior as the insertion of factual information or as propaganda. Government propagation of false information is increasingly common.

Propaganda

The spectrum of cyber statecraft has geopolitical relevance not only through its positive tools of persuasion and attraction. Cyber statecraft is also used by governments and nonstate actors for more punitive intents and the dispersal of misinformation. Vladimir Putin's aggressive behavior epitomizes the exploitation of cyberspace as a propaganda machine. He has used fake Facebook accounts and other well-known social media outlets to depict the Crimean annexation in a positive light. This includes, but is not limited to, falsifying crimes and atrocities committed by Ukrainian extremists. He also has employed the Web to shape the narrative regarding Malaysian Flight 17, providing a range of incredible scenarios ranging from denial that it was shot down to claiming he was the intended target. Similar to how leaders used traditional tools of statecraft in previous eras, he relies on cyber tools to promote a rally-round-the-flag effect and gain domestic support for Russian policy. As in historical examples, Putin applies not just one tool of cyber statecraft but instead integrates cyber propaganda with rising censorship and greater government control of the Internet. China takes a somewhat different approach to online propaganda. The government hires online commentators, often referred to as the 50-cent party, who are paid to participate in online communities to counter anti-party content, promulgate the party agenda, or deter sensitive content.

Violent extremist organizations similarly employ cyber statecraft as a propaganda tool and a key mechanism for recruitment and radicalization. Social media is largely used as the venue for these propaganda instruments. However, some of the more tech-savvy groups, such as Hizballah, have also created apps to recruit followers and disperse their ideologies. Other nonstate groups, such as the Sinaloa Cartel and those linked closely to governments such as the Syrian Electronic Army, similarly create YouTube videos and Twitter accounts as revisionist mechanisms to shape the discourse on current events or to propagate the promise of a luxurious lifestyle as a member of their groups.

Censorship

State use of cyberspace applies to both the manipulation of content, as previously discussed, and the censorship of it. Internet censorship has produced a wide range of outcomes, and the conditions under which it achieves the desired result remain vague. Depending on its depth and breadth, Internet censorship may actually fuel unrest instead of extinguishing it. For instance, Venezuela's attempts in 2014 to censor Twitter only ignited growing protests against the government. Thailand has similarly tried to censor various social media sites, both after protests began last year and after the imposition of martial law. Turkey recently lifted its block on YouTube, which was enacted after recordings of a security meeting were leaked. The subsequent political crisis resulted in increased Internet censorship over the last year, which sparked protests that still plague the Recep Tayyip Erdogan government. Similarly, Rouhani recently banned Instagram, which now joins Facebook and Twitter as an officially banned social media outlet in Iran. Ironically, Rouhani himself is a prolific Instagram user with a large following. Finally, the Serbian government's mismanagement in the wake of some of the country's worst flooding in over a century ignited a vocal cyber backlash. In response, the Serbian government employed censorship to control the narrative, removing sites that highlighted erroneous government actions or were critical of the government writ large.

While the previous examples focus on Internet censorship as a means to limit antigovernment content, China has taken a somewhat different approach, albeit with similar tools. A recent Harvard publication, "How Censorship in China Allows Government Criticism but Silences Collective Expression,"[5] analyzes a wide range of social media data and finds that the major goal of Chinese censorship is to prevent social mobilization. While the previous examples focus on limiting antigovernment rhetoric, Chinese leadership is much more likely to censor any content that may lead to group mobilization, regardless of the topic of the content. This tendency surfaced in 2014 with the 25th anniversary of the 1989 Tiananmen Square Massacre. Chinese censors blocked major social media outlets and references pertaining directly or indirectly to Tiananmen Square, with the objective of preventing any similar social mobilization.

Offensive Cyber Attacks

At the extreme end of the cyber statecraft spectrum, an actor's offensive use of cyber tools rounds out their punitive uses in statecraft. Offensive cyber tools range dramatically in severity and they themselves comprise a broad spectrum of statecraft tools. They could arguably be compartmentalized into four distinct areas: insertion (for example, malware), blocking (distributed denial of service [DDoS]), removal (cyber espionage), and destruction (such as of critical information or infrastructure). In 2009, the United Arab Emirates relied on the partially state-owned telecommunications company Etisalat to request that its BlackBerry users update their phones with service enhancements, which consequently implemented spyware on devices that provided the government with unauthorized access to private information. The pro-government Syrian Electronic Army, a loosely knit group of hacktivists, went even further and has been credited with—among other cyber attacks—the implementation of Dark Comet and Blackshades malware against antigovernment activists. Although the strength of its direct ties to the Bashar al-Asad regime is unclear, the nonstate group does function as a government surrogate and has aimed domestic attacks against antigovernment activists. Many of their tools bear a resemblance to those used by Iran against its population during the Green Revolution, and many analysts believe Syria is using Iranian-designed offensive software. It is possible the Asad regime used similar tools in 2012 during the unprecedented 2-day Internet blackout in Syria.

These examples illustrate the increasing trend of states employing cyber sticks against their own populations. Of course, offensive cyber statecraft is not limited to domestic implementations. Cyber attacks have also clearly become a tool in interstate power politics, evident in conflicts and disputes as diverse as those between North and South Korea, Russia and Georgia, and India and Pakistan. In some of these instances, similar to how the Syrian Electronic Army has perpetrated cyber offense, nonstate groups closely aligned with the state government actually carry out the cyber attack, elevating the complexity of the interstate conflict due to the ambiguous nature of attribution in cyberspace. States certainly have the advantage in implementing highly technical and complex offensive tools such as those used in the Olympic Games, the German-based R2D2 Trojan, and Russian CosmicDuke. Similarly, to date, interstate dynamics maintain a monopoly on the use of destructive cyber tools such as Stuxnet, which damaged Iranian nuclear reactors in Natanz, as well as the Shamoon virus, which attacked the Saudi Arabian oil company Saudi Aramco. Shamoon infected three-quarters of the company's personal computers (PCs), but was stopped before affecting the oil supply. The Aramco attack required the company to replace tens of thousands of its PCs and is believed to have originated from Iran.

Given the asymmetric nature of the cyber domain, these tools do not reside solely in the domain of state actors, although the scale and scope can obviously vary significantly when employed by nonstate actors. Chinese hackers recently stole health records by exploiting the Heartbleed bug, while the Target and Neiman Marcus data breaches are perhaps the most prominent examples of successful cyber espionage aimed at multinational corporations. The decentralized, loosely knit hacktivist group Anonymous has aimed its tools at both state and nonstate groups, carrying out DDoS attacks against the Israeli government and using their cyber exploits to support Arab Spring movements. Nevertheless, governments are countering the group's influence. The British government's DDoS attacks against Anonymous might be the first publicized instance of a state-sponsored DDoS campaign. As these examples continue to surface, each new revelation sets a precedent for a potential rise in offensive cyber statecraft within cyberspace. However, attribution issues escalate the role of misperception within cyberspace, rendering it much more difficult to comprehend the long-term impact that the instantiation of these tools will have on international relations.

Conclusion

This initial overview of a cyber statecraft framework—and the range of tools available to state and nonstate actors—provides a more structured and nuanced approach for exploring and understanding the growing use and implications of cyber statecraft. This is long overdue, as the national security implications of cyber statecraft remain greatly underexplored yet are rising in importance. Cyber as a tool of statecraft has been commandeered by an overemphasis on its militarized aspects. This focus on cyber's offensive manifestations ignores the nuanced nature of this critical domain and its broader application to geopolitics. Although powerful and disruptive, cyber statecraft comprises much more than just intelligence or offensive capabilities. Analysts and policymakers alike must begin viewing cyber statecraft not as a discrete offensive tool useful only in narrow cases, but rather as a form of statecraft on par with other more traditional forms of statecraft, with state and nonstate applications ranging from attraction to coercion along the soft-hard power continuum. Applying a more formalized statecraft model to cyberspace helps add robustness and promote greater comprehension of the role of cyber statecraft for security and policy leaders, while adding to the international relations community's understanding of the national security and geopolitical implications of cyber statecraft and cyberspace writ large.

It is time to end the hyperfocus on cyber as a predominantly offensive tool that is not only inherently destabilizing and exacerbates the security dilemma, but also omits the diverse ways states operate within the domain. The examination of cyber as statecraft would also benefit from increased coordination between the technology and strategic studies communities. The technical nature of this domain is likely one of the causes of the inattention cyber statecraft has received relative to its importance in the international system. Although still in its infancy as a domain, a cyber statecraft framework will enable more holistic thinking about how actors leverage cyberspace and will ideally open the door for future research at the technology-policy nexus, and thus promote an expanded comprehension of the ways in which this technical disruption affects global affairs. JFQ

Notes

[1] Joseph S. Nye, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly 5* (2011), 19.

[2] Jason Healey, ed., A *Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

[3] World Bank, *Information and Communication for Development: Maximizing Mobile* (Washington, DC: The World Bank, 2012).

[4] World Bank, *World Development Indicators* (Washington, DC: The World Bank, 2015), available at <http://data.worldbank.org/products/wdi>.

[5] Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107 (May 2, 2013), available at <http://gking.harvard.edu/files/gking/files/censored.pdf>.

Standard Missile 3 launched from Aegis combat system–equipped USS *Decatur* during Missile Defense Agency ballistic missile flight test intercepting separated ballistic missile threat target (U.S. Navy)

Understanding the Indications and Warning Efforts of U.S. Ballistic Missile Defense

By Thomas K. Hensley, Lloyd P. Caviness, Stephanie Vaughn, and Christopher Morton

It is true today as it was ten years ago that this effort holds the promise of changing the course of human history, by freeing the world from the ominous threat of ballistic missile attack. Given the choice, shouldn't we seek to save lives rather than avenge them?

—President Ronald Reagan on the 10th Anniversary of the Announcement of the Strategic Defense Initiative

The critical mission of defending the U.S. homeland—homeland defense—requires a fully integrated capability to identify, categorize, and fuse strategic and tactical indications and warnings (I&W) by U.S. Strategic Command (USSTRATCOM), North American Aerospace Defense Command (NORAD), U.S. Northern Command (USNORTHCOM), and U.S. Pacific Command (USPACOM). Today's fiscally constrained environment may encourage decisionmakers to eliminate perceived I&W "redundancies" and create an I&W stovepipe for weapons release authorities (WRAs). In a mission area where time is of the essence and failure would result in grave damage to national security, such an arrangement would create an unacceptable risk to homeland defense.

Overview

According to the U.S. Missile Defense Agency, "countries invest in ballistic missiles because they are a means to project power in regional and strategic contexts" and provide "a capability to launch an attack from a distance."[1] This has led to an increase in ballistic missiles over the past 5 years. The total number of these systems outside the United States, the North Atlantic Treaty Organization, Russia, and China has risen to over 5,900.[2] Hundreds of launchers and missiles are currently located within range of deployed U.S. forces.[3]

According to the U.S. Intelligence Community, current trends indicate that ballistic missile systems using advanced liquid- or solid-propellant propulsion technologies are becoming increasingly mobile, reliable, survivable, and accurate, and have the ability to strike targets over longer distances. Moreover, the "proliferation of ballistic missiles is increasing the number of anti-access weapons available to potential regional adversaries. These weapons could be used to reduce military options for combatant commanders and decrease the survivability of regional military assets."[4]

These threats from state actors will likely become more dangerous due to increases in the numbers, capabilities, and lethality of delivery systems and payloads in development. North America currently has a modest BMD system specifically developed to counter intercontinental ballistic missile (ICBM) threats from rogue nations. BMD is a system of systems employing a layered defense architecture.[5] It architecture integrates BMD capabilities and intelligence systems for I&W to defeat ballistic missile threats.[6] Despite the vast array of terrestrial and space-based collection assets designed to provide I&W, however, the Intelligence Community faces challenges with providing strategic I&W. In particular, prioritization of geographic combatant commanders' priority intelligence requirements (PIRs) could potentially create gaps in coverage, affecting timely intelligence that supports WRAs for effective BMD employment. This is important because of the limited engagement timeframe for incoming ballistic missiles from launch to impact. The decision by a WRA to engage must occur within minutes of a launch to enable defeat of the incoming weapon.

Rogue State ICBM Threats to North America

Originally intended to counter the Soviet nuclear threat during the Cold War, BMD technology in the 21st century has shifted focus to defending the U.S. homeland against regional actors such as Iran and North Korea.[7] North Korea's advancements in its existing ICBM inventory and nuclear capabilities are a concern. While Iran does not currently possess an ICBM, Tehran is making tremendous strides in pursuit of ICBM technologies, also creating concerns for the United States.

North Korea continues to advance its existing ICBM arsenal. In December 2012, the North Koreans demonstrated their technological advancements in potentially launching an ICBM by successfully placing a satellite in orbit using an Unha-3 rocket. A variation of the Taepo Dong-2 ICBM, the Unha-3 is a three-stage rocket.[8] North Korea currently possesses two potential ICBM vehicles: the Taepo Dong-2 and KN-08.[9] In March 2013, Joint Chiefs of Staff Vice Chairman Admiral James Winnefeld commented, "We believe the KN-08 probably does have the range to reach the United States."[10] In addition, North Korea has taken steps to develop road-mobile KN-08 launchers, complicating timely I&W prior to launch and thereby creating exceptionally tight timelines for ICBM discrimination and ground-based interceptor (GBI) targeting post-launch.[11]

Currently, the North Koreans do not possess the means to place a nuclear warhead on either of these platforms. However, coupling their ICBM progress with the detonation of a third nuclear device in February 2013, North Korea is either intentionally or unintentionally signaling a desire to develop a capability to threaten North America.[12] As a result, in March 2013, Secretary of Defense Chuck Hagel announced that "the United States would be bolstering its missile defenses."[13]

For the past 60 years, North Korea, with its isolated, authoritarian regime led by a succession of unstable leaders, has been a seemingly intractable and exceptionally dangerous security and stability problem. There are numerous specific examples where Pyongyang's erratic and irrational behavior nearly reignited conflict on the Korean Peninsula. A nuclear-armed North Korea significantly changes the security calculus and the ability of the United States to negotiate with or influence Pyongyang. In April 2012, North Korea changed its constitution, describing the country as a "nuclear-armed nation."[14] In February 2013, Pyongyang threatened South Korea and the United States with a preemptive nuclear strike, further complicating the situation.[15] Whether North

Colonel Thomas K. Hensley, USAF, is Deputy Director of Intelligence at the North American Aerospace Defense Command–U.S. Northern Command. Colonel Lloyd P. Caviness, USARNG, is Chief of Staff–Army National Guard at the Fires Center of Excellence, Fort Sill, Oklahoma. Colonel Stephanie Vaughn, USA, is Deputy Director of the Nuclear Technologies Department at the Defense Threat Reduction Agency. Christopher Morton is an Operations Chief in the National Geospatial-Intelligence Agency.

Korea would actually use nuclear weapons is hotly debated. However, an irrational North Korea equipped with nuclear-armed ICBMs *perceiving* a threat to its regime could result in a serious and dangerous miscalculation that would threaten North America.

Iran does not currently possess an ICBM capability; however, Tehran continues to prioritize and advance its ballistic missile programs. Since the 1980s, Iran has relied on its North Korean and Syrian partners to export and then assist in the development of short- and medium-range ballistic missile systems. Despite its original reliance on third parties, Iran's missile program has evolved over time, demonstrating the engineering and technical expertise necessary to develop missile technologies on its own.[16] In particular, Iran has continued to work on its satellite launch vehicles (SLVs). In February 2009, Iran successfully launched a satellite into orbit using its Safir-2 SLV platform. Since then, it has been working on upgrades for delivering heavier payloads into higher orbits.[17] According to Director of National Intelligence James Clapper, "Iran continues to expand the scale, reach and sophistication of its ballistic missile forces—many of which are inherently capable of carrying a nuclear payload."[18]

The Defense Intelligence Agency assesses that Iran's development of large space launch vehicles demonstrates an intent to develop ICBM technologies. In January 2012, Secretary of Defense Leon Panetta noted that "Iran might be able to develop a nuclear-armed missile about a year or two after developing a nuclear explosive device."[19] The rapid progress of Iranian missile technology and development is changing the minds of many senior leaders who had been skeptical about the future of Iranian ICBM capabilities and ability to threaten North America.[20]

Similar to North Korea, concerns exist regarding an ICBM-equipped Iran armed with nuclear devices. Iran possesses an extensive inventory of short- and medium-range ballistic missiles. Tehran incorporates these missiles in its overall strategy to "deter—and if need be retaliate—against forces in the region, including U.S. forces."[21] An Iran equipped with nuclear-tipped ICBMs would likely extend that strategy to include North America, thereby seriously affecting the U.S. position and leverage against Iran in regional security issues by holding major U.S population areas hostage. Again, any *perceived* threat to the Iranian regime could result in a serious miscalculation.

I&W Capabilities for BMD

To effectively use ground-based interceptors to counter threats, WRAs must have substantial intelligence resources to detect and monitor perceived indicators via analysts and tools that may offer adequate warning. Whether a single source of information or a fusion of multiple sources, I&W intelligence provides time-sensitive information to military commanders or other senior leaders who may authorize a response to an adversarial action or intention. BMD warning is enabled by a layered multisensor architecture that consists of fixed and mobile land-, sea-, and space-based assets located around the world. Future I&W capabilities for BMD will most likely include greater numbers of systems as described, in addition to more technologically robust systems in development. Nevertheless, the U.S. Government has signaled it will also incorporate joint and multinational efforts beyond those that already exist.[22]

Land-based components of the BMD warning system include fixed sites and mobile phased-array radar sensors. Upgraded early warning radars located in Alaska, California, Greenland, and the United Kingdom provide all-weather, long-range tactical warning of ballistic missile launches, including estimated launch and impact points, to the command authority.[23] The Cobra Dane Upgrade is a midcourse radar in Alaska that detects missiles out to 2,000 miles and operates in the L-band radio frequency.[24] The Army Navy/Transportable Radar Surveillance and Control (AN/TPY-2) consists in part of a high-resolution X-band radar primarily deployed in support of U.S. allies in Asia, Europe, and the Middle East; however, it can also provide acquisition and tracking data for the integrated BMD system.[25]

Sea-based components of the BMD warning system include the ship-based Aegis and semi-submersible platform-based radars, which can each detect and provide acquisition and tracking information for the BMD system. The mobile nature of naval platforms allows them to be repositioned around the globe with efficiency to improve BMD detection coverage during heightened tensions within a given region. There are currently 31 cruisers and destroyers based in the Atlantic and Pacific fleets that are fitted with the Aegis BMD system, with an additional two undergoing installation. Aegis Ashore Installations will be located in Romania and Poland as part of the European Phased Adaptive Approach, with an Aegis Ashore test facility in Hawaii.[26] The Aegis system works in conjunction with the Army Navy/Shipboard Phased-Array Radar (AN/SPY-1) S-Band radar and can detect, cross-cue, and track ballistic missiles to provide warning to other regional and national assets.[27] Aside from U.S.-operated systems, Japan purchased Aegis for its four *Kongo*-class guided missile destroyers,[28] and smaller, less capable Aegis versions are carried by Australia, Norway, South Korea, and Spain.[29] Furthermore, the Sea-Based X-Band (SBX) radar is mounted on a twin-hulled, self-propelled drilling platform that is jointly operated by the Missile Defense Agency and Military Sealift Command.[30] Primarily used for BMD testing purposes in the Pacific, the SBX radar can also be deployed in support of homeland defense. The land-, sea-, and space-based sensor systems can provide target track information to the command, control, battle management, and communications (C2BMC) system, which then provides tracking information to other radar systems and track and discrimination information to the shooter systems for organic or remote engagement.

Space-based systems have provided the United States a strategic and tactical I&W capability for more than five

Patriot Advanced Capability–2 missile launcher during crew drill (U.S. Air Force/Nathanael Callon)

decades. The once-classified, second-generation satellite constellation known as the Defense Support Program (DSP) was first launched into orbit in 1970.[31] DSP satellites use short- and mid-wave infrared sensors in a geosynchronous Earth orbit (GEO), allowing constant or near-constant vigilance in support of the overhead persistent infrared mission.[32] The third-generation satellite constellation known as Space-Based Infrared Systems uses a mix of GEO and highly elliptical orbit satellites, which allows for scanning and staring[33] of selectively targeted areas with increased sensitivity as compared to the older DSP satellites.[34]

Future sensors are in development to improve and enhance current BMD warning capabilities. In addition, multinational efforts in the Asian, European, and Middle Eastern regions will become more robust and include nontraditional partners such as China and Russia,[35] suggesting that the United States and its allies perceive North Korea and Iran as the primary antagonists of the ballistic missile threat. These future platforms will enable earlier I&W, which will increase the engagement windows for the BMD systems and provide additional decision timeframes for the WRAs.

Combatant Commander Responsibilities for I&W

Although USSTRATCOM provides subject matter expertise on global I&W for ICBM threats as well as planning and operational issues related to BMD, each geographic combatant commander is responsible for protecting the homeland in the command's respective area of responsibility (AOR). USNORTHCOM and USPACOM have specific roles and tasks within this construct.[36] The USNORTHCOM commander has the overarching responsibility of protecting North America as the supported command, with assistance from USPACOM and NORAD as supporting commands.[37]

The USSTRATCOM commander is responsible for synchronizing global BMD plans and operations, in addition to providing missile warning to

NORAD and other combatant commanders if the appropriate combatant command is unable to do so.[38] To this end, the USSTRATCOM commander established the Joint Functional Component Command for Integrated Missile Defense (JFCC-IMD) as the synchronizing body for the BMD system.[39] The Missile Defense Agency and JFCC for Intelligence, Surveillance, and Reconnaissance support JFCC-IMD in providing "shared situational awareness, integrated battle management C2 [command and control], adaptive planning, and accurate and responsive battle damage assessment."[40]

BMD System

The ballistic missile defense system is a complex, distributed system of five elements (four shooter elements and one C2 element), five sensor systems (four radar systems and one space-based system), and supporting efforts. The integration of these many elements and efforts enable a robust, layered defense against a hostile missile in all phases of flight.[41] The shooter elements include the Aegis BMD, Terminal High-Altitude Area Defense system, Patriot missile defense system, and Ground-Based Midcourse Defense (GMD) system. The sensor systems include the Aegis BMD AN/SPY-1 radar, Cobra Dane radar, upgraded early warning radars, AN/TPY-2 (forward-based mode) radar, and Space-Based Infrared Systems/DSP. In addition, the Sea-Based X-Band radar (primarily a test asset that can be operationally deployed as needed) will be used within the BMD system when available. The command and control element is the C2BMC, a vital operational system that enables the President, Secretary of Defense, and combatant commanders at strategic, regional, and operational levels to systematically plan BMD operations, collectively see the threat develop, and dynamically manage designated networked sensors and weapons systems to achieve global and regional mission objectives.[42] This group of automated systems enables each sensor and shooter to integrate by sharing targeting information and engagement control for a WRA.

The U.S. GMD missile system currently is the only demonstrated capability for defense against ICBM threats to the United States.[43] Planners bin ballistic missiles into one of five categories based on their maximum range capabilities: close range (62–186 miles), short range (under 620 miles), medium range (between 620 and 1,800 miles), intermediate range (between 1,800 and 3,400 miles), and intercontinental (greater than 3,400 miles).[44] For ICBM threats to the United States, the BMD system relies on GBIs launched from U.S. bases to intercept and kill the missile or warhead during the midcourse phase of its flight. (GBIs are the only system available to attack an ICBM during this phase.) The United States currently has GBI silos at Fort Greely, Alaska, and Vandenberg Air Force Base, California.[45]

Ground-based interceptors are three-stage, solid-fueled boosters with an exoatmospheric kill vehicle (EKV). Upon ICBM launch detection and recognition as a threat to the United States, a WRA can launch GBIs in self-defense. The decision to launch must be made with enough time available for the GBI to reach the ICBM during the midcourse phase. During the GBI flight, the EKV separates from its booster and uses onboard sensors for target detection, guidance, and discrimination, resulting in a collision with the targeted reentry vehicle while it is still in its midcourse phase.[46]

ICBMs have three stages of flight: boost, midcourse, and terminal. The boost phase begins with the launch of the missile/warhead and lasts until the rocket engine burns out, approximately 3 to 5 minutes.[47] The midcourse phase, which is the longest phase of flight, starts after rocket engine burnout and continues with the missile/warhead exiting Earth's atmosphere, reaching its apogee, and beginning its descent, and can last up to 20 minutes.[48] During the terminal phase of flight, the detached warhead reenters Earth's atmosphere and continues until detonation or impact. This generally lasts less than a minute.[49] In total, the three stages of ICBM flight last less than 30 minutes. During this time, a WRA must identify the ICBM launch, determine if the launch is a threat to the United States, decide to engage the ICBM with GBIs, and achieve a successful kill while the missile is still in its midcourse phase of flight. Currently, the BMD system relies on intelligence and sensors to indicate the construction or deployment of rogue nation systems to provide warning of an impending attack. This additional time allows for deployment of additional radar sensors toward the anticipated launch site in order to detect and track any incoming missile.

Integrated Threat Analysis: Current Situation

A number of factors degrade effective strategic I&W, creating a particularly dangerous situation with respect to the North Korean ICBM threat and timely WRA response for BMD employment. First, North Korea is an isolated, closed state that denies robust, comprehensive intelligence collection operations. As a result, the Intelligence Community relies on nonpersistent, space-based imagery collection for North Korea.[50]

Second, these nonpersistent, space-based assets are in high demand, especially by coalition commanders focused on the Korean Peninsula. The capabilities needed for BMD I&W are shared with other PIRs, such as North Korean long-range artillery; short-, medium-, and intermediate-range ballistic missiles; and ground, air, and air defense forces.

Third, even when these space-based assets are used to collect information on North Korean ICBMs, the road-mobile threats, combined with North Korean camouflage, concealment, and deception efforts, make them extremely difficult to find and track. Thus, it is conceivable that the first indication of a North Korean ICBM launch against North America would come from tactical I&W from overhead persistent infrared assets, starting the clock for a WRA to make a GBI engagement decision.

According to Joint Publication 3-27, *Homeland Defense*, and the Unified Command Plan, it is incumbent upon

Oscar-01 launch control facility missile trailer at Whiteman Air Force Base, MO (U.S. Air Force)

USPACOM, USNORTHCOM, and USSTRATCOM to use the I&W resources in their toolkits to warn against ballistic missile threats.[51] Regional assets, such as Aegis cruisers and destroyers, fixed early warning radar sites, and mobile radar systems, provide information to the combatant commanders for I&W. The President has delegated weapons release authority to USNORTHCOM, precluding USSTRATCOM from WRA for engaging targets.[52] These combatant commander responsibilities reinforce the necessity of I&W and BMD system capabilities within the combatant command to ensure timely response and engagement of all BMD threats to the United States.

Conclusion and Recommendations

Ballistic missile defense is a no-fail mission that requires an interdependent and complementary effort to generate and track strategic and tactical indications and warning intelligence. It is imperative that leaders understand the importance of the BMD system and component systems to ensure continued funding for these systems and I&W platforms. This will reduce the chances of creating stovepipe systems that cannot (or are slow to) communicate with other systems. In a mission area where time is of the essence and failure would result in grave damage to national security, failure to support the BMD system would create an unacceptable risk to homeland defense. It is also imperative that we continue to improve and grow I&W capabilities for BMD throughout the combatant commands.

Although USSTRATCOM is responsible for synchronizing global I&W for ballistic missile threats, USNORTHCOM, along with USPACOM, requires its own organic I&W capability for BMD for four primary reasons. First, a USNORTHCOM ballistic missile defense I&W element, specifically focused on ICBM threats to the homeland, can collaborate with USPACOM, USSTRATCOM, and the Intelligence Community to leverage the imagery collection resources for strategic I&W of the Pacific region, primarily North Korea. Without this focused attention and emphasis, other commands may weight collection efforts more toward peninsula-focused PIRs, especially during times of increased tensions, and thereby create gaps in collection coverage.

Second, a USNORTHCOM BMD I&W element, in close collaboration with USSTRATCOM and USPACOM and focused on tracking strategic I&W developed by monitoring ICBM activity on the Korean Peninsula, would exponentially increase overall situational awareness of North Korean preparations and intentions for launching an ICBM. Strategic I&W is critical in order to position other mobile platforms as well as to prepare the BMD system, should indications show a North Korean desire and readiness to launch.

Third, should North Korea launch an ICBM against North America, a USNORTHCOM BMD I&W element could ensure that the intelligence-to-shooter is properly communicated in a timely manner to the USNORTHCOM commander. Upon notification of a launch, the commander has only a few minutes from launch identification to determine if it is a threat to North America and to successfully engage the threat.

Finally, due to limited time and resources, actions and reactions to a missile launch must be flawless, especially among geographic combatant command areas of responsibility. The entire system must work as one unit despite its geographically distributed parts. To aid in the effective handoff of BMD responsibilities between AORs, shared, pristine situational awareness is paramount. North Korean intent is evident. Ballistic missile defense of the homeland is a no-fail mission that starts with collaborative and timely strategic and tactical I&W provided by USNORTHCOM, USPACOM, and USSTRATCOM. JFQ

Notes

[1] "The Threat," Missile Defense Agency Fact Sheet, December 2014, available at <www.mda.mil/system/threat.html>.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Bernard Ulfers and George LeFurjah, "AN/SPY-1B/D RADAR Design Changes Supporting Aegis Ballistic Missile Defense," *Leading Edge* 7, no. 2 (2013), 101.

[6] Ibid.

[7] Jonathon Masters and Greg Bruno, "U.S. Ballistic Missile Defense," Council on Foreign Relations Backgrounder, May 2006, available at <www.cfr.org/defensehomeland-security/us-ballistic-missile-defense/p30607>; Joint Publication (JP) 3-27, *Homeland Defense* (Washington, DC: The Joint Staff, 2009), III-18.

[8] Frank Harvey, *North Korea, Ballistic Missile Defence, and Canada-US Defence Cooperation*, Canadian Defence and Foreign Affairs Institute (CDFAI) Policy Paper (Calgary, AB: CDFAI, 2013), 1, 5, available at <www.cdfai.org/PDF/North Korea Ballistic Missile Defence.pdf>.

[9] Greg Thielmann, *Sorting Out the Nuclear and Missile Threats from North Korea* (Washington, DC: Arms Control Association, 2013), 6, available at <www.armscontrol.org/files/TAB_Sorting_Out_North_Korea_2013.pdf>.

[10] Ibid., 7.

[11] Ibid., 3, 6.

[12] Ibid., 1.

[13] Richard Weitz, "US Missile Defense: Closing the Gap," *World Affairs Journal* (July–August 2013), 80, available at <www.worldaffairsjournal.org/article/us-missile-defense-closing-gap>.

[14] Emma Chanlett-Avery and Ian Rinehart, *North Korea: U.S. Relations, Nuclear Diplomacy, and Internal Situation*, R41259 (Washington, DC: Congressional Research Service, 2013), 6, available at <www.fas.org/sgp/crs/nuke/R41259.pdf>.

[15] Ibid., 1.

[16] Chris Smith and Matthew Wallin, "Iranian Ballistic Missiles," *AmericanSecurityProject.org*, August 2013, 1, available at <http://americansecurityproject.org/featured-items/2013/fact-sheet-iranian-ballistic-missiles/>.

[17] Ibid., 5.

[18] Masters and Bruno, 6.

[19] Kenneth Katzman, *Iran: U.S. Concerns and Policy Responses* (Washington, DC: Council on Foreign Relations, 2012), 36, available at <www.cfr.org/iran/crs-iran-us-concerns-policy-responses/p282737>.

[20] Smith and Wallin, 6.

[21] Katzman, 36.

[22] *Ballistic Missile Defense Review Report* (BMDR) (Washington, DC: Department of Defense, February 2010), v–vii.

[23] "Upgraded Early Warning Radar," Missile Defense Agency Fact Sheet, April 2013, available at <www.mda.mil/global/documents/pdf/uewr1.pdf>.

[24] "Cobra Dane," Missile Defense Agency Fact Sheet, February 2013, available at <www.mda.mil/global/documents/pdf/cobradane.pdf>.

[25] "Army Navy/Transportable Radar Surveillance (AN/TPY 2)," Missile Defense Agency Fact Sheet, February 2013, available at <www.mda.mil/global/documents/pdf/an_tpy2.pdf>.

[26] "Aegis Ballistic Missile Defense," Missile Defense Agency Fact Sheet, August 2013, available at <www.mda.mil/system/aegis_bmd.html>.

[27] Ronald O'Rourke, *Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress*, RL33745 (Washington, DC: Congressional Research Service, 2011), 2–3, available at <https://opencrs.com/document/RL33745/>.

[28] "Aegis Ballistic Missile Defense."

[29] O'Rourke, 3.

[30] "Sensors," Missile Defense Agency Fact Sheet, November 2012, available at <www.mda.mil/global/documents/pdf/sbx.pdf>.

[31] "Defense Support Program: Satellites," U.S. Air Force Fact Sheet, February 2, 2011, available at <www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5323>.

[32] Ibid., 1.

[33] "The two basic types of focal plane arrays are scanning and staring. The simplest *scanning* device consists of a linear array. An image is generated by scanning the scene across the strip. . . . A *staring array* is the two-dimensional extension of a scanning array. It is self-scanned electronically, can provide enhanced sensitivity, and is suitable for lightweight cameras [emphasis added]." See Lester J. Kozlowski and Walter F. Kosonocky, "Infrared Detector Arrays," 33.6–33.7, available at <www.mhprofessional.com/handbookofoptics/pdf/Handbook_of_Optics_vol2_ch33.pdf>.

[34] "Infrared Space Systems Directorate," U.S. Air Force Fact Sheet, November 23, 2011, available at <www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5330>.

[35] BMDR, 31–35.

[36] JP 3-27, *Homeland Defense*, II-18.

[37] Ibid., III-17–III-19.

[38] Ibid., III-19.

[39] Ibid., III-18–III-19.

[40] Ibid.

[41] "A System of Elements," Missile Defense Agency Fact Sheet, July 18, 2013, available at <www.mda.mil/system/elements.html>.

[42] "Command, Control, Battle Management, and Communications (C2BMC)," Missile Defense Agency Fact Sheet, November 2012, available at <www.mda.mil/system/c2bmc.html>.

[43] Baker Spring, "Protecting U.S. Territory Against Long-Range Missiles: Second Approach Needed," Heritage Foundation Issue Brief #3987, July 15, 2013, available at <www.heritage.org/research/reports/2013/07/protecting-us-territory-against-long-range-missiles-2nd-approach-needed>.

[44] Masters and Bruno, 1–2.

[45] Ibid., 4.

[46] Weitz, 83.

[47] Robert G. Gard and Kingston Reif, "Fact Sheet: U.S. Ballistic Missile Defense," Center for Arms Control and Non-Proliferation, 2013, available at <http://armscontrolcenter.org/issues/missiledefense/articles/fact_sheet_us_ballistic_missile_defense/>.

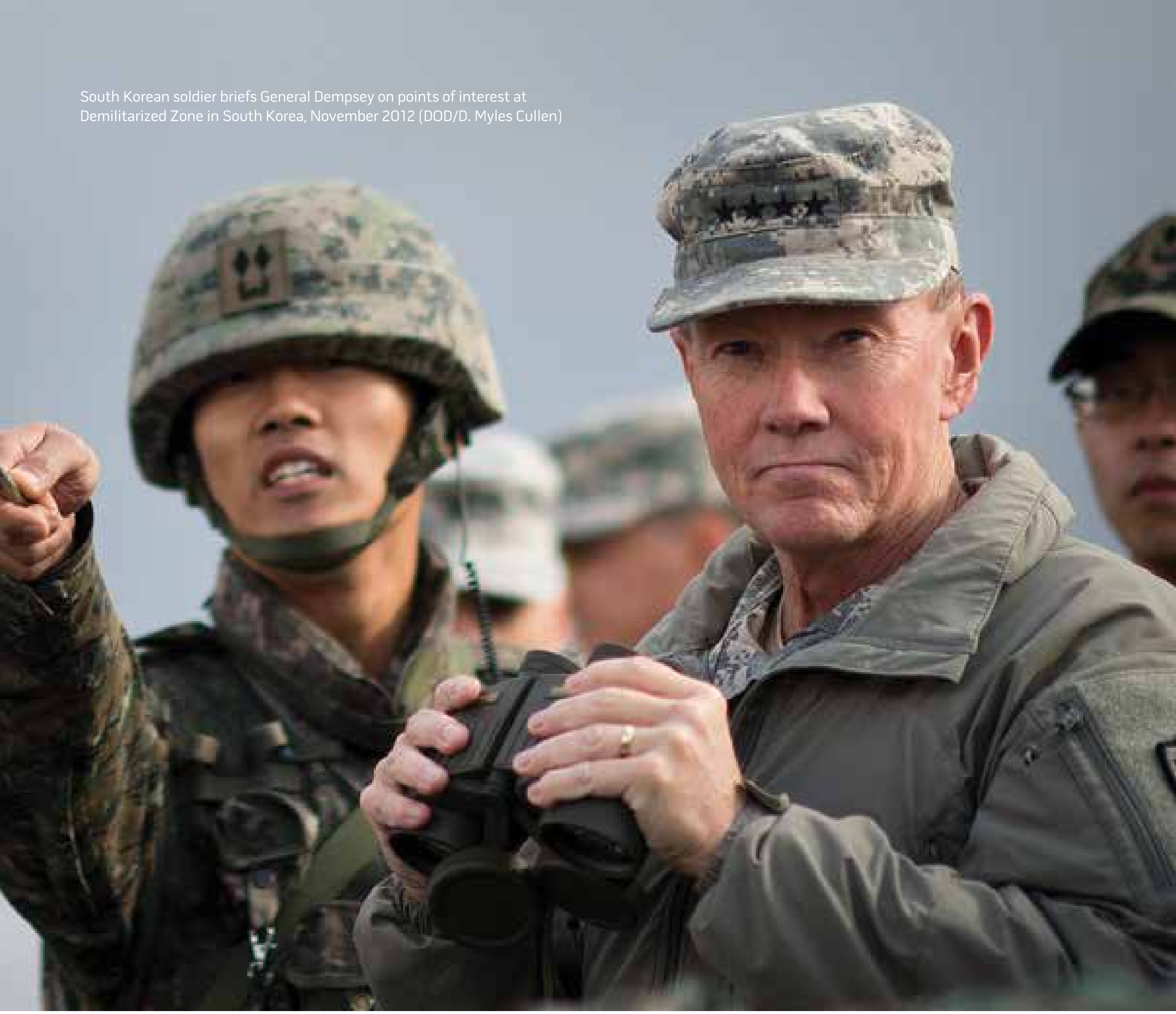
[48] Ibid., 1.

[49] Ibid.

[50] JP 3-14, *Space Operations* (Washington, DC: The Joint Staff, January 6, 2009), V-5–V-6.

[51] JP 3-27, *Homeland Defense*, II-9, II-12, III-13.

[52] Ibid., III-19.



South Korean soldier briefs General Dempsey on points of interest at Demilitarized Zone in South Korea, November 2012 (DOD/D. Myles Cullen)

Spinning the Top

American Land Power and the Ground Campaigns of a Korean Crisis

By John Johnson and Bradley T. Gericke

Lieutenant General John "JD" Johnson, USA, is Director of the Joint Improvised Explosive Device Defeat Organization. Colonel Bradley T. Gericke, USA, currently serves on the Army Staff.

Gashed from the yellow earth and scarred by lacerating wire bound to steel posts, the moment Korea's Demilitarized Zone (DMZ) comes into view, you cannot avoid the impression that you are witness to a crime. In a way, you are. The DMZ is an ominous wound from an unfinished conflict dividing the Korean Peninsula and serving as a boundary between incarceration and freedom. It carves its way between Korea's sharp-sloped green hills only 20 short miles from the megacity of Seoul and its surrounding environs with its 25 million people who, after decades of economic development, are enjoying increasingly prosperous lives. The DMZ both signifies suffering already endured and foreshadows violence yet to come. It represents a status quo inter-bellum, which cannot endure. It is like no other place in the world. And the complex strategic and operational challenge that it poses to America's joint force is likewise daunting.

The fact that war has not yet returned to the Korean Peninsula is in large measure due to U.S. security assurance. In close and enduring partnership with the armed forces of the Republic of Korea (ROK), American military power has to date tempered hostilities and assured all actors that the cost of military ambition would be high. By no means, however, is the tumultuous history between the states and peoples of this critical region finished, nor should the absence of major war in recent decades be seen as a diminished mandate for U.S. military deterrence, shaping activities, and operational readiness.

In every so-called balance of power, stability is a constructed outcome that puts competing interests in suspension. Stability is not an accident, and it requires active intervention to endure. Like spinning a top, sustained intervention in the form of applied force is necessary to keep the thing going. If the top loses its spin, equilibrium is lost. For more than 60 years that force has been applied in Korea on the ground by American troops. They have been Northeast Asia's key guarantors of stability. They have kept the top spinning.[1]

But now a young leader sitting atop the North Korean regime threatens anew what has become fashionable to blink at: escalatory conflict on the Korean Peninsula. The standoff there is not simply a relic of the Cold War or a quaint regional affair whose consequences can be held distant from American shores. The implications for American security and prosperity are global and increasingly urgent. War in Korea would inflict a terrible toll, and the United States could not avoid the butcher's bill.

For the joint force, and for the U.S. Army in particular, a clear-eyed consideration of the high-intensity demands of a 21st-century war in Korea is overdue. We must be clear about the fundamental nature of a war waged on the Korean Peninsula. A centerpiece of U.S. joint campaigns would be a ground war—American boots on the ground in Asia. And those ground forces, as members of a joint force in partnership with our ROK ally, would be called on not only to prosecute multiple, often simultaneous operations to achieve the essential military objectives necessary to defeat North Korean military forces, but also to secure the North's weapons of mass destruction (WMD) and the enabling components of WMD networks, facilitate the delivery of humanitarian assistance to the population, and assure order to set the conditions for the return of civil authority. Thus, if war erupts, it would be extraordinarily complex and dangerous.

Accomplishing these tasks would require much of our Armed Forces. In addition to the layered threats posed by the North's armed forces, the deeply isolated political and economic character of the North Korean state means denial of air and sea environments alone would be necessary and enabling, yet not sufficient to the prosecution of a campaign on the peninsula. Land dominance would be essential to military success.[2]

The Strategic Environment

While not recently in the forefront of military planning, Asia is a familiar battleground. The United States is a Pacific nation, with our country's political, economic, and security interests tightly bound to this dynamic region. Since 1898, the United States has waged four major Pacific conflicts—the Philippine Campaign (1899–1913), World War II (1941–1945), Korean War (1950–1953 and through today), and Vietnam War (1962–1972)—as well as numerous smaller scale operations and deployments. Despite the common perception that the Pacific is an air-maritime theater, since 1898 the U.S. Army has waged more ground campaigns in the Pacific than anywhere else in the world. Likewise, Asian states have themselves fought ground wars, and with sizeable forces. The Army's attention to this theater is historically rooted in genuine posture and readiness demands.[3]

As each of the Services seeks to balance worldwide commitments in an era of domestic fiscal constraint, the effects of posture decisions will be felt in the Korean theater. In concert with Army choices, the stationing or rotational presence of Navy ships, Air Force strike aircraft, and Marine forces will matter greatly. The time it takes to bring U.S. capabilities to bear in the event of conflict becomes an enemy itself if joint capabilities are moved farther from the Korean Peninsula.

North Korea's violent provocations and bombastic pronouncements that have ratcheted up tensions in recent years mark a familiar recurrence in the constructed, public confrontations so necessary to the North. The regime capably underpins its diplomacy through a double-bind approach that generates a political crisis to set conditions, followed by facile concessions to reset conditions *ante*, underpinned with the threats posed by an industrial-scale WMD program and improving missile delivery systems.

North Korea is a security-first state.[4] Perpetual tension with South Korea (and the United States) is the raison d'être for the North Korean regime. Manufactured vexation directed against the South and the United States is employed to justify the hardships imposed on the North Korean people by the North's leaders. These leaders are not irrational—but they do not see the world as the West does, either. Why would they hazard a war? One

Republic of Korea and U.S. Soldiers at Demilitarized Zone in South Korea face North Korea (DOD/D. Myles Cullen)

catalyst would be the perceived threat posed by the West to regime leadership. Readiness—and the sacrifices demanded by the public to stay ready—to fight to protect the ethnic Korean nation whose only true defender is the North is inherent to their ruling ideology. North Korea's leaders comprehensively prioritize a military mindset and act accordingly.[5] Their ambition to protect the North's self-declared concept of Korean racial and cultural purity means that the regime cannot go far down the path of economic reform and political liberalism. The elasticity that Western policymakers seek from the regime is simply incompatible with that mindset. This does not mean the North's rulers are martyrs, but it does leave plenty of decision space to risk a war, even if they could be defeated eventually. It is better to remain firmly in control and resist for as long as possible than to incur the high risk posed by instability.

It is axiomatic that North Korea's leaders see their own authority as an existential issue and would have little interest in restraint in defending themselves. They would employ every tool at their disposal to preserve their regime: conventional forces, special operations capabilities, cyber attacks, missile and artillery volleys, and, logically, WMD. The U.S. joint force must not presume that the selective application of U.S. weapons in an attempt to limit the scope of the conflict would be feasible. Once its ruling elites see themselves in jeopardy, North Korea could be expected to fight with all its capabilities. The fates of recent U.S. adversaries such as Muammar Qadhafi, Saddam Hussein, and even Bashar al-Asad are surely near to mind; none serves as models for paths to accommodation with the United States. Thus U.S. and ROK military planning must admit that North Korea's leaders are motivated to protect their interests. That translates to war across the range of military operations, against a determined adversary, in Asia—complexity posing severe challenges for American planners.

The North's aggressive promotion of confrontation also heightens the risk of unintended consequences such as an escalatory spiral driven by emotion, miscalculation, and chance. It is entirely feasible—in fact most likely—that any major military engagements would start with little or no notice. The scenarios for escalation are remarkably complex and merit a clear-eyed consideration of the kind of campaigns likely to be waged in crisis. In all cases military action would certainly be many things: fast-paced, violent, fought in multiple domains, high risk, and international in scope. What it would *not* be is easily limited or waged only on American terms.

Here is where U.S. policy desires and the shadow of history collide. Common wisdom asserts that another war on the Korean Peninsula is, in effect, unthinkable. Regional stakes are too high. Too many global powers and their economies are in play. Enormous populations are at risk. At home, an American public and policy class is weary from a decade of war in the Middle East. The default then is to hold the prospect of war in Asia at arm's length while hoping for time to remuster American military strength and for something—anything—to change on the Korean Peninsula that leads to an end-of-Cold-War–style soft landing. But given North Korea's record, one should hold little optimism for a negotiated settlement to conclusively lessen tension on the peninsula.[6] It is a risky proposition to assume that the relatively orderly endgame of the Cold War in Europe would be replicated in northeast Asia. The history is simply different, and so are the cultures in play.

It should not be surprising then that the North's leaders appear to be sticking to their playbook. Their March 2010 sinking of the ROK *Cheonan*, with the loss of more than 40 ROK sailors, and the shelling of Yeonpyeong Island in November of that year, the largest military assault against the South since the armistice, are provocations very much in the North's customary style. Then in April 2012, North Korea launched a 90-ton Unha-3 rocket ostensibly for the purpose of placing a satellite in orbit but likely serving as a test platform for long-range missile technologies. (It is in this context that the alleged cyber attacks by North Korea against Sony in late 2014 must be understood.) And of course even more seriously, the North has claimed several successful underground nuclear tests in recent years. Leaders in Pyongyang no doubt see little incentive to try a new approach so long as their longstanding approach of provocation followed by extraction of concessions continues to work. This is especially true now, as Kim Jong-un tightens his authority through assassination of his political rivals in a rare third-generation hereditary transition within an autocratic state.

In the meantime, change is under way south of the DMZ, which further heightens military risk. The population of South Korea is justifiably proud of hard-earned prosperity, and while they long tolerated provocations by the North, that forbearance is now being sorely tested.[7] The public made their displeasure known by reacting with revulsion to the civilian loss of life as a consequence of the Yeonpyeong shelling. In the years since, the public's perception of their security has declined significantly.[8] ROK political leaders have taken note. After each of the North Korean provocations in 2010, senior ROK leaders were dismissed, including ministers of defense, the chairman of the joint chiefs of staff, and a number of general officers. The result is that the armed forces are more determined and readier than ever to deliver a prompt, firm, and unequivocal military response in the event of another such North Korean attack. This is just the kind of tinder that could spark a broader conflagration.

A salutary development at the level of national policy is that the U.S. Department of Defense is beginning the rebalance of force capabilities to the Asia-Pacific region.[9] In addition, the U.S. Army, despite its ongoing commitments in the Middle East, has recently published its operating concept, *Win in a Complex World*, with its embedded idea of "joint combined arms operations." Such operations consist of "synchronized, simultaneous, or sequential application of two or more arms or elements of one service, along with joint inter-organizational and multinational capabilities to ensure unity of effort and create multiple dilemmas for the enemy."[10] The Army's concept proposes the kind of integrated, adaptable maneuver that would be necessary to confront and then defeat likely adversaries in any theater, but seems highly suited to the diverse challenges posed by North Korea.

The Operational Environment

If wars really do end in the mud, then the physical environment of northeast Asia offers plenty. Korea's weather is extreme—brutally humid and monsoonal in the summer and bitterly cold in the winter. Most of the peninsula features rugged, compartmented terrain characterized by low-lying rice paddies and farm fields with steeply sloped mountains. U.S. mobility would be challenged. Logistical support would be severely tested. In short, the Korean Peninsula presents considerable challenges that would test U.S. troops and equipment.

The military resources available to the North are more formidable than they may at first appear. Despite their aging equipment, inadequate transport, outdated communications gear, and poor maneuver training, they retain significant lethal capabilities. While conquest of the peninsula may no longer be feasible—a fact that the North's military leaders likely understand—the North's armed forces pose multiple, in-depth, and complex challenges to U.S. and ROK armed forces.[11] The North Koreans would still be a formidable adversary in ground combat and possess strategic and operational attack options via robust short-, medium-, and long-range missile and cannon capabilities, which alone could put at risk most of the ROK's population. North Korea's armed forces are the fourth largest in the world, including an active-duty strength of more than 1.2 million—at least twice the size of the South's.[12] The North does not possess the professional officers and modernized equipment of the South, but the regime's military leadership is indoctrinated and loyal, and the North Korean People's Army (NKPA) boasts both large numbers of armored vehicles and an especially lethal indirect fire inventory: 7,500 mortars, 3,500 towed artillery pieces, 4,400 self-propelled cannons, and 5,100 multiple-rocket launchers. These can deliver both standard high explosives and chemical munitions.

Swiftly neutralizing a large number of delivery systems is problematic even for U.S. and ROK forces that possess decided qualitative advantages. And of course, North Korea has declared itself to be nuclear-weapons capable. Interrupting and then rendering safe whatever nuclear materials do exist is a wicked problem.[13] Thus the counter weapons of mass destruction (CWMD) mission set plays a regular and prominent role for U.S. Army forces on the peninsula. The prospect of waging war with conventional means against a nuclear-capable foe would itself constitute a new chapter in modern warfare, one whose implications deserves extensive scrutiny.

With these capabilities, the North could launch indirect-fire raids against key ROK cities and U.S. military installations while deploying large numbers of its 60,000-strong special operations forces (SOF) across the peninsula, and conduct limited objective incursions to seize key terrain south of the DMZ for use as negotiating leverage later. Such an offensive would pose a potent combination that would be difficult to repel. The North's battlefield dispositions pose a challenge much more akin to the conditions at Verdun than the rapid offensive of 1950. This is not to say that the NKPA could not conduct limited attacks and seize terrain; it likely could. But the army's strength comes from waging a defensive struggle, inflicting ROK and U.S. casualties, panicking the large population of Seoul, buying time for its national leadership to employ asymmetric weaponry and to press for an early diplomatic accommodation that leaves the regime intact.

South of the DMZ, Koreans today are justifiably proud of their economic success and protective of their hard-won affluence that has witnessed the explosive growth of a middle class in recent years.[14] One result is a deeper calculation by the South of the intersection of its economic and security interests. Trade and defense issues between South Korea, China, Japan, and the United States are deeply intertwined. Even as the South and the United States continue to negotiate force posture issues and matters of operational control of forces within their alliance framework, the military partnership remains resilient and strong. In fact, U.S. troop levels in Korea have stabilized after several years of drawdown, and the U.S. Army is modernizing and improving readiness of its forces stationed on the peninsula.[15] The ROK army is a highly motivated force that is earnestly modernizing and would fight hard. But it is also a force that is challenged to perform offensively with the speed and alacrity of U.S. forces. South Koreans and our allies in the region expect that the U.S. Armed Forces would fulfill alliance obligations and would carry a hefty share of the warfight. To do less would irreparably damage U.S. prestige, risk U.S. interests in the region, and likely exacerbate human suffering.

A Three-Campaign Land War

Two frequently encountered assumptions about war on the peninsula are that the war would move lockstep up the peninsula, phase line by phase line in a replay of 1950–1953, or that conflict would be limited to a specific piece of terrain, waged primarily by select—standoff—military platforms. We should employ greater imagination and resist the temptation to believe that the adversary would allow U.S and ROK forces to march the length of the peninsula as the North succumbs to "shock and awe." While U.S. precision strike capability is certainly a good thing, it just would not be enough because the nature of the war would reflect the totality of its objectives.[16] It would be fought in checkerboard fashion, with ground, sea, air, and cyber operations occurring simultaneously. Central to the contest would be the need to seize and hold ground.

For U.S. forces, the burden of waging war would fall first on U.S. Forces Korea (USFK), a subunified command that also shoulders the responsibility of representing the United Nations as the United Nations Command and partner to the ROK as it contributes to the bilateral Combined Forces Command.[17] USFK troops and arriving joint forces from the region and the continental United States would be required to wage three broad campaigns: neutralize North Korea's offensive WMD capability and protect the capital of Seoul (existential and immediate), secure WMD sites and defeat North Korean conventional and unconventional forces (existential and essential); and conduct WMD site exploitation and stability functions to aid the population and enable ROK-led reunification of the peninsula under a responsible civilian authority (conflict termination). The operational space in which these missions must be performed would be chaotic, friction would dominate, and U.S. forces would meet resistance in all domains.

The timeline from steady state to the outbreak of crisis would likely be a short one. There is little reason to believe that there would be accurate information regarding North Korean intentions. With ambiguity dictating the opening phases of a crisis, the ability of ROK and U.S. policymakers to make timely decisions would be hampered, compressing the time available for military preparations. Our recent experience in the Middle East would hinder us in Korea. U.S. forces have historically been accustomed to generating combat power over time from largely sheltered operating bases that could receive, equip, and sustain the onward-moving tactical echelons. Even when expeditionary packages are deployed, they are not large and they too benefit from an extensive support network that is protected in the theater. Our forces in Korea would be both at immediate risk and in high demand.

Operational risk climbs quickly over time if necessary capabilities are lacking. The requirements would not only be ordinary classes of supply but would also consist of specialized formations and often highly technical equipment, again demanding ready access if they are to be employed effectively. The distance between Seoul and Los Angeles is about 6,000 miles—a long way to ship or airlift heavy reinforcements, and a trip that would simply take too long if the right mix of capabilities is not already accessible to commanders. At the onset of crisis, ground forces would face the prospect of several major tasks: evacuation of noncombatants out of tactical harm's way (likely more than 175,000 persons), and the reception, staging, and integration of follow-on forces from all Services to the peninsula. These alone are monumental undertakings that would require dedicated manpower and consume that most precious commodity, time. And then, when conflict erupts, U.S. forces would confront a threat posing complexity and scale unlike any combination faced elsewhere in the world.

In the face of this threat, the first campaign to command the attention of the world's capitals would be to render neutral North Korea's strategic weapons and associated capabilities, especially nuclear weapon launch and detonation. In 2006, the North publicly declared that it had conducted a successful underground nuclear test, and 3 years later it claimed to possess a nuclear weapon. No doubt it continues to pursue nuclear weapons capability, the only purpose of which could be to hold its neighbors and adversaries hostage, including the United States. In the interim, the North is ambitiously developing a range of missile technologies and platforms, some of them near fielding and possibly already in low-rate production, which could enable it to strike farther into the depth of the peninsula and as far as Japan.

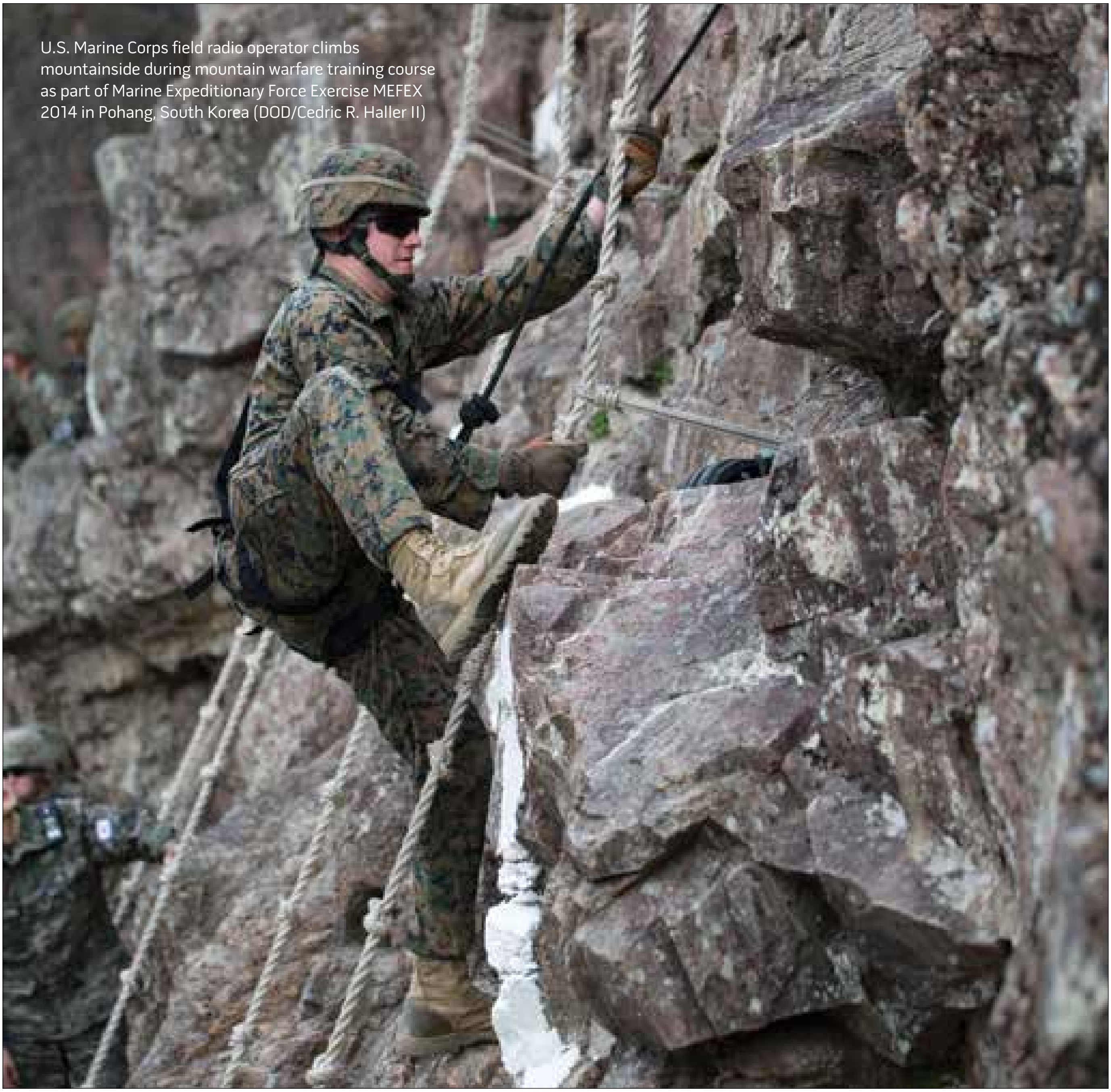
Taking down the North's strategic and operational strike weapons capability would include eliminating its ability to perform centralized command and control. The regime, being the center of gravity of the North Korean state, would remain a viable political reality only as long as it could provide centralized control. However, as we have seen in the Middle East in recent years, this does not mean that violence is terminated. Lack of central authority can in fact serve as an accelerant, which leads to the next challenge.

The next component of the ground campaign would be to wage a fight that in some respects resembles the battlefields of Northern France in 1918 as much as a 21st-century fight: lots of artillery, lots of chemical weapons, and large numbers of dug-in forces. One urgent aspect of this conventional fight is the ROK determination—and U.S. obligation—to protect the city of Seoul and its environs. There is little doubt that the North would launch a massive artillery and rocket barrage if it is afforded the opportunity to do so. Vigorous measures from the ground, sea, and air would be necessary to stymie the North's indirect fire attacks.

U.S. Army Prepositioned Stock IV receives upgraded Bradley Fighting Vehicles as ongoing effort to strengthen readiness across Korean Peninsula (U.S. Army/Bryan Willis)

Elsewhere north of the DMZ, uniformed troops and regime security forces would likely continue to fight, whatever the status of the central regime in Pyongyang. They would almost certainly follow their "last orders" and resist until they are killed or unable to offer any resistance. At the same time, North Korean SOF, highly trained and well equipped by the regime and one of the largest special operating formations in the world, would pose a significant threat. These purpose-built organizations are intended to open a "second front" behind the allied lines—in both South Korea and North Korea—and could be expected to achieve considerable disruptive effect. Alongside the officially sanctioned SOF, armed bands inspired either through deprivation and hope of food or gain or simply out of desperation and fear of ROK and U.S. troops could be expected to resist vehemently in northern areas. North Korean arsenals and underground facilities near the border area no doubt number in the hundreds, replete with munitions and explosives that could easily be turned into improvised explosive devices.

Finally, it is inevitable that ground forces must to some extent participate in stability operations, particularly during the transition following offensive combat operations. While the ROK would formally take on the requirement to establish a competent government authority to initiate the reconstitution of civic functions and services in the North, U.S. forces would inevitably be required to pacify chaotic conditions on



U.S. Marine Corps field radio operator climbs mountainside during mountain warfare training course as part of Marine Expeditionary Force Exercise MEFEX 2014 in Pohang, South Korea (DOD/Cedric R. Haller II)

the ground. A critical mission within this environment is for the Army to lead joint force efforts on the ground to perform CWMD missions.[18] Harnessing the full suite of capabilities of the joint force to address the WMD threat would be a necessary and demanding priority that would influence nearly every aspect of ground operations. This is a central feature of the Korean Peninsula's warfighting environment and one with worldwide implications for U.S. forces.

WMD: New Missions on the Ground

The North's extensive WMD architecture has matured to the point that it is now a dominating feature of the Korean battlespace. It endangers civilian populations and military forces on the peninsula, and it puts in harm's way, either by deliberate use or even as a result of an accidental release, every neighboring state. Once the North is denied the ability to employ these weapons, their elimination—their isolation and ultimate destruction—poses the next inevitable and important step for U.S. forces in conjunction with our ROK allies. There is no U.S. agency with the requisite mission command and robust means to protect friendly forces and allies on the ground—and with the requisite special skills—other than U.S. Army forces enabled by joint capabilities.

The precise number, function, and location of the North's WMD sites and associated installations are not known. The North keeps its programs shrouded in secrecy. Thus U.S. and ROK forces would undoubtedly discover many facilities that are currently hidden. Joint CWMD operations would constitute a WMD "movement to contact" as our formations gain contact with the adversary's network and construct a more accurate and comprehensive picture of the threat. Operations would require specific chemical, biological, radiological, nuclear, and explosives–trained and –equipped personnel and units at every echelon.[19]

The U.S. strategy for combating WMD contains several components, including nonproliferation, counterproliferation, and consequence management. WMD-elimination operations are both technically demanding and manpower-intensive actions to systematically locate, characterize, secure, disable, or destroy WMD programs and related capabilities, each of which is manpower intensive.[20] There is no substitute for trained and ready forces on the ground to perform these necessary mission tasks.

In Summary

During the intervening six decades since the 1953 Korean Armistice Agreement, the divide between North and South—in effect between the past and the future—has only deepened. This disparity is increasingly perilous as the regime in the North depends ever more exclusively on its military-political complex for its survival. It lacks international legitimacy and possesses only a fractured and declining economy, and its people have been starved, slaughtered, brainwashed, and coerced into submission.

In a region featuring important U.S. national interests, the persistent presence of American forces and capabilities, in close partnership with the Republic of Korea and regional partners, has kept war at bay. How much longer this balance (the spinning top) can be kept in play cannot be known. The severe rigidity of the North Korean political-military nexus and the potential for miscalculation that such a system engenders renders any balance of power inherently unstable.

Defeating North Korea militarily would require the joint force to operate in every domain. The land campaign would be decisive. In every eventuality, among key U.S. objectives is that the North Korean WMD program must be rendered safe. If crisis erupts in Korea, American military forces on the ground would be central actors to safeguard U.S. interests and restore stability. JFQ

Notes

[1] For a short quote from Secretary of State Henry Kissinger concerning balances of power, see Niall Ferguson, "America's Global Retreat," *Wall Street Journal*, February 21, 2014.

[2] Lukas Milevski, "*Fortissimus Inter Pares*: The Utility of Landpower in Grand Strategy," *Parameters* (Summer 2012), 9.

[3] Andrew Bacevich, "The Endless Army: Is 'Pacific Pathways' a Necessary Pivot or Military Budget Grab?" *Boston Globe*, January 10, 2014.

[4] The crimes of the North Korean regime against its own people are increasingly well documented, adding further pressures to regime decisionmaking. See "Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea," United Nations Office of the High Commissioner for Human Rights, February 2014.

[5] See B.R. Myers, "Planet Pyongyang," Newsweek, April 15, 2013. See also B.R. Myers, *The Cleanest Race: How North Koreans See Themselves and Why It Matters* (New York: Melville House, 2010). Professor Myers's book offers a penetrating assessment of the North Korean regime's ideology.

[6] Provocations of course are longstanding features of North Korean behavior. In the mid-1960s the North initiated more than a decade of violent acts along the Demilitarized Zone (DMZ) that took dozens of lives. Major terrorist actions included a raid to assassinate the South's president, Park Chung-hee, at his official residence in the Blue House in Seoul (1968); seizing the U.S. naval vessel USS *Pueblo* (1968); and the murder of two U.S. Army Officers in the DMZ (August 18, 1976).

[7] Karl Friedhoff, "South Korean Public Opinion Following North Korea's Third Nuclear Test," Public Opinion Studies Center, The Asan Institute for Policy Studies, March 8, 2013. For the South's immediate response in 2010, see Keith B. Richburg, "South Korean President Takes Responsibility for Failing to Protect Country, Signals Hardened Military Stance Toward North," *Washington Post*, November 29, 2010.

[8] Karl Friedhoff, "How South Koreans View National Security," *Wall Street Journal–Asia*, April 11, 2013.

[9] Secretary of Defense Leon Panetta in David Alexander, "U.S. Will Put More Warships in Asia," Reuters, June 2, 2012.

[10] *The U.S. Army Operating Concept: Win in A Complex World*, U.S. Army Training and Doctrine Command Pamphlet 525-3-1, October 7, 2014, 45.

[11] Alexandre Y. Mansourov, "North Korea: Turning in the Wrong Direction," *38North.org*, April 2013, available at <http://38north.org/2013/04/amansourov041013/>.

[12] Anthony Cordesman et al., *The Korean Military Balance: Comparative Korean Forces and the Forces of Key Neighboring States* (Washington, DC: Center for Strategic and International Studies, 2011), 40.

[13] Regarding North Korean nuclear weapons effects on select Republic of Korea targets, see Bruce W. Bennett, "Deterring North Korea from Using WMD in Future Conflicts and Crises," *Strategic Studies Quarterly* (Winter 2012), 125.

[14] "South Korea: EU Bilateral Trade and Trade with the World," DG Trade Statistics, March 21, 2012.

[15] Raymond T. Odierno, "The U.S. Army in a Time of Transition: Building a Flexible Force," *Foreign Affairs,* May–June 2012.

[16] Not discussed in this article are the enabling operations to be waged in cyberspace and space, or other instruments of national power such as economic sanctions or blockades. Nor discussed are the prominent roles to be played by key powers in the region, to include Russia, Japan, and prominently, China.

[17] About 20,000 of the 28,000 troops stationed in Korea are U.S. Army Soldiers. It is already fashionable among the military intelligentsia to charge that the Air-Sea Battle concept will trump the imperative of U.S. Army forces in Asia. The facts on the ground speak differently. For a short review of the debate among the Services, see Sydney J. Freedberg, Jr., "The Next War," *Government Executive Magazine*, August 15, 2012.

[18] See Joint Publication (JP) 3-40, *Countering Weapons of Mass Destruction* (Washington, DC: The Joint Staff, October 31, 2014).

[19] "White Paper," U.S. Army 20th Support Command (CBRNE) [chemical, biological, radiological, nuclear, and explosives], Background Information, September 2011.

[20] JP 3-40, A-1.

Soldiers of 91st Brigade Engineer Battalion, 1st Brigade Combat Team, 1st Cavalry Division, prepare to breach road block set up by opposition forces during exercise Combined Resolve II at Joint Multinational Readiness Center in Hohenfels, Germany, May 2014 (U.S. Army/Nicholaus Williams)

Making Soup with Stones

JMTC Partnership and the NATO Connected Forces Initiative

By John G. Norris and James K. Dunivan

First published in Europe in 1947 by Marcia Brown after World War II, many children have grown up reading a classic story titled "Stone Soup." Most of us are probably familiar with this tale, based on French folklore, of three hungry and tired soldiers approaching a village where the peasants hid their meager rations of food upon learning of their approach. In a wily and enterprising solution, the soldiers begin boiling a large pot of water in the town square as they profess to make soup from three small stones. The people of the village, impressed by this notion, begin contributing bits and pieces of meat and vegetables to create a meal for everyone, thus highlighting the power and importance of cooperation and what small contributions by all can produce for the greater good.

The overarching theme of this story still resonates today, particularly among North Atlantic Treaty Organization (NATO) countries. During the 50th

Colonel John G. Norris is Commander of Operations Group and the Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany. Lieutenant Colonel James K. Dunivan is Brigade Senior Trainer at JMRC.

anniversary of the Munich Security Conference on February 1, 2014, then–Secretary of Defense Chuck Hagel outlined "renewed and enhanced" partnership and cooperation with NATO as a fundamental component of our National Security Strategy:

> *In reviewing U.S. defense priorities, tempered by our fiscal realities, it's clear that our military must place an even greater strategic emphasis on working with our allies and partners around the world. . . . The United States will engage European allies to collaborate more closely, especially in helping build the capabilities of other global partners. We're developing strategies to address global threats as we build more joint capacity, joint capacity with European militaries. In the face of budget constraints here on this continent, as well as in the United States, we must all invest more strategically to protect military capability and readiness. The question is not just how much we spend, but how we spend together. It's not just about burdens we share, but opportunities, as well.*[1]

This idea not only sustains the marriage of cooperation the United States has developed for the past 12 years with the International Security Assistance Force (ISAF) in Afghanistan, but also provides an endorsing reminder for Smart Defense outlined by NATO Secretary General Anders Fogh Rasmussen at the 2011 Munich Security Conference. During his keynote address, aptly titled "Building Security in an Age of Austerity," the Secretary General invoked the Alliance to recognize Smart Defense—"how NATO can help nations to build greater security with fewer resources but more coordination and coherence"—as a means to prudently maintain and improve our collective security in a resource constrained environment.[2]

One year later the Secretary General identified the Connected Forces Initiative (CFI) as a critical component and example of Smart Defense:

> *Smart Defence is about acquiring the necessary capabilities. Connectivity is about making these capabilities work together most effectively. The Connected Forces Initiative mobilises all of NATO's resources to strengthen the Allies' ability to work together in a truly connected way. This is particularly important as we wind down our combat operations in Afghanistan at the end of 2014. I see three areas to focus our efforts in the coming years: expanded education and training; increased exercises, especially with the NATO Response Force; and better use of technology.*[3]

These three important focus areas of CFI are complementary to Secretary Hagel's defense priorities of collaboration and building joint capacity with our European Allies.

These three focus areas are also manifested within the U.S. Army Chief of Staff Strategic Priorities. These tenets of developing "Adaptive Army Leaders for a Complex World," sustaining "A Globally Responsive and Regionally Engaged Army," and maintaining "A Ready and Modern Army" provide nested and necessary guide posts for future operations and engagements, particularly for a Combat Training Center (CTC).[4] To that end, the leaders and Soldiers of the U.S. Joint Multinational Training Command (JMTC) headquartered at Grafenwoehr, Germany, to include the Joint Multinational Readiness Center (JMRC) at Hohenfels, have worked tirelessly to "make soup" with these "three stones" that comprise the CFI and advance the intent of our Army and national defense leadership.

Education and Training

The JMTC, especially throughout the past decade, has been instrumental in preparing U.S. and multinational units for service abroad in operations in Iraq, Afghanistan, and Kosovo. The state-of-the-art facilities and equipment, maneuver area, and most importantly its proximity to allied and partner nations in Europe have made the JMTC an affordable, accessible, and economical location of choice to train, validate, and certify coalition units to enable their operational success.

Proximity does not directly equal access, however, so the JMTC uses the "3P" approach to developing partnership—persistence, patience, and presence. Once trust, confidence, sincerity, and respect are achieved at all levels of engagement, the access we acquire enables effective training and presents more training opportunities. This access promotes mutual understanding and greater interoperability among soldiers and leaders. Brigadier General Walter Piatt, the JMTC commander, likes to remind us that "Nations do not have relationships, people do. We gain credibility through shared hardship."[5]

Global challenges have offered ample occasions to share hardship, but as the United States and NATO prepared to conclude the ISAF mission at the end of 2014, the Alliance is expected to shift its emphasis from operational engagement to operational preparedness. This presents an unprecedented opportunity for education and training with our European partners at JMTC. We can continue to capitalize on the relationships and sustain the partnerships established during a time of war, but with latitude to shift from an operational environment–specific "readiness exercise" to a decisive action "leadership laboratory" with first-class, realistic training against a near-peer competitor tailored to specific objectives and desired outcomes.

While a majority of partnered education and training occurs at JMTC, a tremendous amount of this effort occurs on the home soil of our allied and partner nations. Enabled by geographical proximity, a majority of our senior experienced trainers travel to various countries to conduct leader training programs, specialty training, training center development, and military-to-military cooperation events. This expeditionary capability and ability to export our training expertise has greatly strengthened our partnership with other nations, both reinforcing the U.S. Army Europe (USAREUR) and U.S. European Command (USEUCOM) key task of Theater Security Cooperation and, perhaps demonstrated more tangibly, enabled U.S. and multinational

Reservist with 6250th U.S. Army Hospital watches for injured Soldiers during mission at U.S. Army's 7th Army Joint Multinational Training Command's Grafenwoehr Training Area, Germany, July 2014 (U.S. Army/Christina M. Dion)

units to "enter the box" at a higher level of training readiness when operating together in the field.

An increased level of training readiness obviously contributes to a more successful outcome. More important, completion of a capstone training event that complements home-station training and offers an opportunity to work with other Alliance or partner nations allows units to demonstrate their national capabilities while increasing interoperability, readiness, and collective security. A premier manner to accomplish all of these objectives is through participation in a multinational and multi-echelon named exercise.

Exercises

Exercises in Europe and the JMTC are nothing new—they have been successfully executed for many years under such auspices as the Joint Chiefs of Staff exercise program. What is unique—and enabled by geographical proximity and personal partnership in Europe—is JMTC's eagerness and initiative to use an exercise construct to increase multinational interoperability and mission command, which are vital components of NATO's vision of Smart Defense and CFI in achieving enhanced collective security.

In November 2013, the JMTC conducted Exercise Combined Resolve, which was designed as a proof of principle for the European Rotation Force and focused on improving NATO interoperability (nine different nations) by integrating warfighting functions, personnel, and doctrine, while integrating the USEUCOM Army Contingency Response Force company to demonstrate our ability to rapidly mobilize and integrate our forces across a theater of operations to support our allies with a responsive combat force.

Following Army Chief of Staff guidance to Combat Training Centers as a design framework, Combined Resolve also established a standard for future exercises at JMRC. Leader development was paramount as we transitioned from assessing readiness to a focus on leaders at all levels training their subordinate commands. Special operations forces (SOF)–conventional force interdependence was not only maintained, but the inclusion of multinational SOF from France also demonstrated the interoperability required for coalition warfare. JMTC inculcated an expeditionary mindset as the forces from all countries operated out of tactical assembly areas in the austere German winter environment, while leveraging force structure challenges of working with nonorganic enablers such as National Guard engineers, U.S. Close Combat Aviation, and fires provided by Czech Republic Artillery while receiving support from a limited logistics footprint. Finally, the entire exercise scenario exemplified a dynamic operational environment as forces trained in force-on-force missions ranging from combined arms maneuver to wide area security.[6]

Adding to the complexity of the operational environment, the active participation of our multinational partners during Combined Resolve demonstrated a positive example of the benefits of CFI and fulfilled the NATO Secretary General's goal of bringing together "modern, tightly connected forces, equipped, trained, exercised, and commanded so that they can operate together, and with partners, in any environment."[7]

Given the unparalleled success of this exercise, JMTC began the process of planning Combined Resolve II for May 2014. This exercise, focusing on Army Chief of Staff guidance to support development of responsive forces, will continue as a multinational training event that expands upon the interoperability lessons learned during Combined Resolve I. This iteration will include live-fire gunnery and more force-on-force

Soldiers provide cover for bounding troops during exercise Combined Resolve III, October 2014, in Grafenwoehr, Germany (U.S. Army/Marcus Floyd)

training days to truly test the rigors of multinational brigade operations and sustainment in a decisive action environment. Fifteen countries and over 3,000 personnel—including the European Response Force from Fort Hood, Texas, as well as numerous joint, multinational, and National Guard partner states—are scheduled to participate in this exercise, making it one of the largest multinational exercise events ever to be hosted at JMTC.

Technology

Given the strong interest and recognized value in conducting multinational exercises, JMTC is working to use technology to expand these training events beyond JMTC to allow multi-echelon training across a connected domain throughout Europe. There are many aspects of technology that drive interoperability and Smart Defense, many of which are beyond the JMTC sphere of influence. Relative to our focus within CFI, however, is leveraging technology to build on our dedication to realistic training and increased exercises that stress enhanced interoperability and NATO compliance. Accordingly, JMTC is developing an initiative to harness network and simulation technology to enable "Connected Training."

Currently, JMTC supports individual training to collective training, soldiers to brigades, in exercises that blend live, virtual, and constructive events. At the division level and three-star headquarters, JMTC events focus on using both virtual and constructive realms. Technology enables JMTC to conduct exercises that integrate allied forces based in various global locations and has been demonstrated in numerous named regional exercises such as Saber Strike, Saber Guardian, and Saber Junction. Under the auspice of Connected Training, JMTC is now pursuing the capability to conduct simultaneous live exercises that are distributed among partner CTCs throughout Europe.

A majority of USEUCOM and USAREUR partner nations have established fully operational and capable

Combat Training Centers with live, virtual, and constructive capabilities. These national CTCs have a unique range of capabilities to host sizable simulated command post exercises with maneuver space to support company- to battalion-level training, as they are modeled and equipped similar to JMTC. They are also an excellent way to minimize training costs as they allow many countries to train at home station or in a neighboring country. This dramatically cuts the costs associated with travel and shipment of large pieces of military equipment as it is cheaper to "push electrons" within a Connected Training network.

Reduced costs for training will undoubtedly lead to continued expansion of the network and larger exercises in support of CFI. Building on years of security cooperation and numerous military-to-military partnership-training events, USAREUR and USEUCOM now have the ability and the capacity to integrate or "connect" a larger number of our allied forces into their training exercises. Furthermore, the opportunity to connect regionally in a distributed environment is no longer limited to the tactical level. We have the capability to connect the tactical to operational level command with a corps headquarters, establishing a joint operations center at the Joint Multinational Simulations Center in Grafenwoehr to control and "fight" the distributed exercise. At the JMRC in Hohenfels, a multinational brigade headquarters conducts a live exercise with subordinate battalions, companies, or adjacent brigade headquarters located at JMTC partner CTCs throughout Europe.

During the post-ISAF environment paradigm shift of emphasis from operational engagement to operational preparedness, the timing and opportunity are right to fully implement and explore the capability of Connected Training. This could serve as an ideal training model for NATO and Allied Land Command as it looks to train its nine NATO Rapid Deployment Corps and the contributing nations of the NATO Response Force, allowing the Alliance to further enhance responsible readiness and collective security. Vigorous exploration and application of Connected Training will build on the success of previous training and exercises while sustaining multinational partnerships and interoperability with our Allies, which will ultimately fulfill the intent defined by Smart Defense and the CFI.

Stirring the Pot

None of this will be easy. In his successful book *Learning to Eat Soup with a Knife*, John Nagl begins by addressing T.E. Lawrence's aphorism that "Making war upon insurgents is messy and slow, like eating soup with a knife. . . . It is difficult to fully appreciate until you have done it," he writes in the foreword, "Intellectually grasping the concept . . . is a different thing from implementing the measures required to do it."[8] The same can be said for JMTC partnership and the CFI.

Over the past year, however, the JMTC has fully committed its time, energy, and resources to achieving success "soup" with the three "stone" focus areas of education and training, exercises, and technology. There is more to be accomplished as we expand partnership and pursue technology to fully enable Connected Training, but we are on glide path to achieve irreversible momentum toward realizing the full potential of the CFI and its implications for Smart Defense. The associated gains in collective security for the Alliance with interoperability and increased readiness to face future contingencies and challenges to that security make it all worthwhile.

With NATO CFI as a desired end-state—or waypoint—our ability to move forward will continue to depend on a willingness to apply "blood and treasure" to JMTC. With only two U.S. Brigade Combat Teams in Europe, there may be a natural disposition to assume a robust training center is not required on this continent. However, as long as policy developers and decisionmakers view JMTC as a strategic capability within Europe, with a scope that extends beyond the training and readiness of our own U.S. forces, then a convincing argument can be made that JMTC is a notable "stone soup" that Alliance partners can season. In a resource-constrained environment in particular, the Connected Training opportunities that are afforded by JMTC, with prime proximity and years of productive partnership, are a viable and prudent direction to pursue.

As then-Secretary Hagel noted in Munich, "The challenges and choices before us will demand leadership that reaches into the future without stumbling over the present."[9] While no one can accurately predict the region, type, or scope of the next conflict, most can agree that agile and adaptive readiness is essential for collective security. If we clearly identify with the vision set out by the former Secretary of Defense in maintaining NATO as "the centerpiece of our transatlantic defense partnership," then the present JMTC initiatives contributing to CFI will continue to extend our security reach for generations to come. JFQ

Notes

[1] Chuck Hagel, Remarks at the 2014 Munich Security Conference, Munich, Germany, February 1, 2014.

[2] North Atlantic Treaty Organization (NATO) Secretary General Anders Fogh Rasmussen, Keynote Address at the 2011 Munich Security Conference, Munich, Germany, February 4, 2011.

[3] NATO Secretary General Anders Fogh Rasmussen, Remarks at the Allied Command Transformation Seminar, Munich, Washington DC, February 28, 2012.

[4] General Raymond T. Odierno, Chief of Staff of the Army, "Waypoint #2," February 21, 2014.

[5] Brigadier General Walter Piatt, USA, commander, U.S. Joint Multinational Training Command, Combined Resolve Final Brigade Combat Team After Action Report Notes, November 25, 2013.

[6] Raymond T. Odierno, "Transformation of the Combat Training Centers," September 4, 2013.

[7] NATO Secretary General Anders Fogh Rasmussen, Remarks at the NATO Defence Ministers Meeting, Brussels, Belgium, October 22, 2013.

[8] John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: University of Chicago Press, 2005), xi–xvi.

[9] Hagel.

Led by RB-66 Destroyer, pilots flying Air Force F-4C Phantoms drop bombs on communist military target in North Vietnam, August 1966 (U.S. Air Force)

The Limits of Airpower or the Limits of Strategy

The Air Wars in Vietnam and Their Legacies

By Mark Clodfelter

For most of the world's population, America's air wars in Vietnam are now ancient history. The first U.S. bombing raids against North Vietnam, conducted in response to attacks by North Vietnamese patrol boats on the destroyer USS *Maddox* in the Tonkin Gulf, occurred a half-century ago this August. Seven months later, America began its longest sustained "strategic bombing" campaign, Operation *Rolling Thunder*, against the North. That effort, and the *Linebacker* campaigns that followed, dropped a million tons of bombs on North Vietnam. Three million more tons fell on Laos and Cambodia—supposedly "neutral" countries in the conflict. Four million tons fell on South Vietnam—America's ally in the war against communist aggression. When the last raid by B-52s over Cambodia on August 15, 1973, culminated American bombing in Southeast Asia, the United States had dropped more than 8 million tons of bombs in 9 years.[1] Less than 2 years

Dr. Mark Clodfelter is a Professor of Military Strategy at the National War College.

In May 1967, Air Force F-100 Super Sabre fires salvo of rockets at jungle target in South Vietnam (U.S. Air Force)

later, Cambodia, Laos, and South Vietnam were communist countries.

Did the inability of bombing—and innumerable airlift and reconnaissance sorties—to prevent the fall of South Vietnam demonstrate the limits of airpower, or did it reveal that the strategy that relied heavily on airpower's kinetic application to achieve success was fundamentally flawed? From the perspective of 50 years after the bombing began, and 40 years after the last bomb fell, the answer to both questions remains *yes.* Yet the two questions are intimately related, and answering them reveals the enormous impact that a political leader can have on the design and implementation of an air strategy, especially in a limited war. Ultimately, Vietnam demonstrates both the limits of airpower and the limits of a strategy dependent on it when trying to achieve conflicting political goals. The legacies of the air wars there remain relevant to political and military leaders grappling with the prospects of applying airpower in the 21st century.

The reliance on airpower to produce success in Vietnam was a classic rendition of the "ends, ways, and means" formula for designing strategy taught today at staff and war colleges worldwide. Airpower was a key "means" to achieve the desired "ends"—victory—and *how* American political and military leaders chose to apply that means to achieve victory yielded the air strategy they followed. Much of the problem in Vietnam, though, was that the definition of *victory* was not a constant. For President Lyndon Johnson, victory meant creating an independent, stable, noncommunist South Vietnam. His successor, President Richard Nixon, pursued a much more limited goal that he dubbed "peace with honor"—a euphemism for a South Vietnam that remained noncommunist for a so-called decent interval, accompanied by the return of American prisoners of war (POWs).[2]

Yet those definitions of *victory* were only partial definitions of the term. They defined the *positive* political objectives sought—those that could be achieved only by *applying* military force. Equally important, though, were the *negative* political goals—those achievable only by *limiting* military force. To achieve true victory in Vietnam, *both* the positive *and* negative objectives had to be obtained—a truism for any conflict. That challenge was enormously difficult for American political and military leaders in Vietnam because the negative goals often appeared to have an equal, if not greater, weight than the positive goals, especially during the Johnson era of the war.

Johnson's Use of Airpower in Vietnam

President Johnson had a multitude of negative objectives that prevented him from applying massive military force in Vietnam. While he did not intend to lose "that bitch of a war" in Southeast Asia, he also had no intention of surrendering "the woman [he] really loved," the Great Society programs aimed at reducing poverty and achieving racial equality.[3] Achieving the Great Society became an important negative objective for Johnson, one that would prevent him from applying extensive military force. Doing so, he feared, would cause the American public to turn away from the Nation's disadvantaged to focus instead on its military personnel in harm's way. Johnson further feared that applying too much force against North Vietnam would cause its two large allies, China and the Soviet Union, to increase their assistance to the North, possibly even with overt intervention. As a U.S. Senator on the Armed Services Committee, he had seen firsthand what could happen when American leaders miscalculated regarding China during the drive to the Yalu River in the Korean War, and he aimed to prevent a similar mistake in Vietnam. Finally, Johnson was concerned about America's worldwide image, with the globe seemingly divided into camps of communism and capitalism. Exerting too much force against North Vietnam would make the United States appear as a Goliath pounding a hapless David, and likely drive small nations searching for a benefactor into the communist embrace.

Those negative objectives combined to produce an air strategy founded on gradual response, particularly for President Johnson's bombing of North Vietnam. American political and military leaders believed that they had to defeat North Vietnam to stop the insurgency in the South and create a stable government there. Although they knew that the indigenous Viet Cong contributed more manpower to the enemy's cause than did the North Vietnamese army (NVA), they also believed that the Viet Cong (VC) could not fight successfully without North Vietnamese assistance. Accordingly, they designed an air strategy that gradually increased pressure on the North, allowing President Johnson to gauge reactions from the Chinese, Soviets, American public, and other global audiences while he slowly opened the bombing spigot. *Rolling Thunder* would creep steadily northward until it threatened the nascent industrial complexes in Hanoi and Haiphong, and North Vietnamese President Ho Chi Minh, being a rational man who certainly prized that meager industry, would realize the peril to it and stop supporting the Viet Cong. Denied assistance, the insurgency would wither away, and the war would end with America's high-tech aerial weaponry providing a victory that was quick, cheap, and efficient.

Those assumptions provided the foundation for President Johnson's air strategy against North Vietnam, and all of them were seriously flawed. Battles such as Ia Drang and Khe Sanh, as well as the Tet Offensive, were anomalies during the Johnson presidency; for most of his time in office, the Viet Cong and their North Vietnamese allies rarely fought at all. Together, they fought an average of *one day a month* from 1965 to 1968, and as a result, their external supply requirements were minimal. VC and NVA forces in August 1967 numbered roughly 300,000, of whom 250,000 were Viet Cong. Yet that combined force needed only 34 tons of supplies a day from sources outside of South Vietnam—an amount that just seven 2½-ton trucks could carry and that was less than 1 percent of the daily tonnage imported into North Vietnam.[4] No amount of bombing could stop that paltry supply total from arriving in the South. Still, in fighting an infrequent guerrilla war, the VC and NVA could cause significant losses. In 1967 and 1968, 2 years that together claimed 25,000 American lives, more than 6,000 Americans died from mines and booby traps.[5]

For President Johnson, the real problem was translating the application of military force into a stable, noncommunist South Vietnam, and doing so in a way that minimized American involvement and the chances of a broader war with China or the Soviet Union while also maximizing American prestige on the world stage. While airpower had seemed an ideal means to accomplish those ends, in truth it could not do so. The original *Rolling Thunder* raids in March and April 1965 bolstered the morale of many South Vietnamese who desired a noncommunist government, but the South's government was in shambles. After enduring seven different regime changes—including five coups—in 1964, South Vietnam's political leadership faced another crisis on the eve of *Rolling Thunder*, delaying the start of the air campaign by 2 weeks before a semblance of order returned to Saigon. The governments that followed—those of presidents Nguyen Cao Ky and Nguyen Van Thieu—were corrupt and out of touch with the Southern populace.[6] No amount of American airpower could sustain such regimes. Indeed, less than 6 weeks after the start of *Rolling Thunder*, National Security Advisor McGeorge Bundy advised President Johnson that South Vietnam would fall to the Viet Cong if Johnson did not shift the focus of America's military involvement to ground power. The President ultimately concurred, and in summer 1965 he embarked on a program that increased American troop totals from 75,000 to more than 200,000 by the end of the year, with further escalations to follow.[7] The shift in emphasis from airpower to ground power preserved the Saigon government, but did little to assure that it governed competently.

Yet Johnson never completely abandoned his hope that airpower might yield success. In the summer of 1966, he ordered the bombing of oil storage facilities in Hanoi and Haiphong, convinced that trucks were vital to move North Vietnamese men and supplies south and that gasoline was essential to keep the trucks moving. The attacks destroyed

President Nixon meeting with Henry Kissinger in the Oval Office, October 8, 1973 (CIA/Oliver Atkins)

much of the North's oil facilities but failed to affect the pace of the war. A year later, believing that the loss of North Vietnam's meager electrical power production capability and its one steel mill and single cement factory would affect not only its ability to fight but also its will to do so, Johnson bombed those targets. The war continued as it had before, even after intrepid Air Force pilots destroyed the mile-long Paul Doumer Bridge in Hanoi in August 1967. In short, airpower could not affect the outcome of the conflict as long as the VC and North Vietnamese chose to wage an infrequent guerrilla war—and as long as American political leaders chose to back the inept government in Saigon. The rationale for bombing the North became to "place a ceiling" on the magnitude of war that the VC and NVA could wage in the South.[8] That goal faded into oblivion with the opening salvos of the January 1968 Tet Offensive, which demonstrated that American bombing could not prevent the VC and NVA from stockpiling enough supplies to sustain a series of massive conventional attacks.

Despite the failure of Operation *Rolling Thunder* to achieve success, Johnson monitored it closely and tightly constrained actions that American aircrews could take over the North. His negative objectives led to a long list of rules of engagement (ROE) that did everything from preventing flights through the airspace over Hanoi or Haiphong without his personal approval to limiting how closely aircraft could fly to the Chinese border. Many of those restrictions stemmed from his "Tuesday lunch" sessions at the White House, during which Secretary of Defense Robert McNamara, Secretary of State Dean Rusk, National Security Advisor McGeorge Bundy (or Walt Rostow after 1967), and Press Secretary Bill Moyers (and often joined by Johnson cronies such as lawyers Clark Clifford and Abe Fortas) met with the President to select *Rolling Thunder* bombing targets following lunch on Tuesday afternoons. Not until October 1967—after *Rolling Thunder* had been underway for more than 2½ years—did a military officer sit in regularly on the lunch sessions, when Johnson asked Army General Earle Wheeler, the Chairman of the Joint Chiefs of Staff, to begin a steady attendance.[9]

The political restrictions that Johnson placed on the air war over North Vietnam caused military commanders tremendous difficulty in implementing *Rolling Thunder*, but those constraints were not the only ones they had to overcome. Indeed, military leaders developed their own restrictions that limited airpower's effectiveness. Probably the most onerous of those self-inflicted wounds was the "Route Package" system created in spring 1966 that divided North Vietnam into seven bombing zones. Ostensibly developed to deconflict the multitude of Air Force and Navy sorties in North Vietnamese airspace, the system soon became a warped way to assess which Service seemingly contributed more toward *Rolling Thunder*'s effectiveness. The Navy received four of the bombing zones, while the Air Force received the other three. Targets in the Navy zones were off-limits to Air Force fighters without approval from the Navy, and those in the Air Force zones were forbidden for Navy aircraft without permission from the Air Force. Such approvals rarely occurred.[10] As a result, a competition developed between the Air Force and Navy to determine which Service could fly the most sorties into enemy airspace.[11] Much as "body count" became the measure of success for commanders on the ground, "sortie count" became the measure of success for air commanders and often led to promotions. Perhaps the most egregious examples of competition occurred during the bomb shortage of 1966, when increased bombing had expended much of the surplus ordnance from World War II and the Korean War. To maintain the desired sortie rate, Air Force and Navy pilots flew missions with less than a full load of bombs, thereby endangering more aircrews than necessary.[12] One Navy A-4 pilot even attacked North Vietnam's famous Thanh Hoa Bridge with no bombs at all, having been told to simply strafe the structure with 20-millimeter (mm) cannon fire.[13]

"Operational controls" amplified the effects of *Rolling Thunder*'s political and military constraints. Those controls included such factors as environmental conditions and enemy defenses. The North Vietnamese were masters of camouflage and carefully obscured the highways and trails used to send troops and supplies south. Many of those roads were extremely difficult to identify to begin with, given the dense jungle vegetation that covered much of the country. Meanwhile, the North Vietnamese supplemented their deception techniques with an extensive air defense system that guarded lines of communication and the cities of Hanoi and Haiphong. The Soviet Union provided much of the North's hardware, including SA-2 surface-to-air missiles and MiG fighters. By 1966, many analysts considered Hanoi the world's most heavily defended city, an assessment that most Air Force fighter pilots would certainly have endorsed.[14]

In contrast to the limited inputs that American military leaders had in selecting targets in North Vietnam, in South Vietnam the military chiefs faced relatively few political restrictions. President Johnson and his advisors deemed that raids against enemy positions in the South would provoke only minor reactions from the Chinese or Soviets, and that the strikes condoned by Southern leaders on their own territory would produce a meager outcry from the American public or world community. Such attacks required approval only from the South Vietnamese province chief who was responsible for the welfare of those living in his province. Yet obtaining that approval did not guarantee a successful mission. American commanders were often uncertain of enemy positions and bombed "suspected" staging areas. In particular, American and South Vietnamese troops created "free fire zones" where they removed the populace and declared that anyone found in the area was hostile.[15] The people traversing the zones, though, were often innocent villagers trying to return to their ancestral homes. Raids against such areas that killed civilians inspired hatred against the United States and the Saigon regime and made excellent recruiting vehicles for the Viet Cong. In the effort to win so-called hearts and minds and enhance the stability of the Saigon government, the airpower applied over South Vietnam was frequently a double-edged sword.

Whereas the air war over North Vietnam was a conflict for control waged between the Air Force and Navy, the air war over the South was an even more disparate affair. An array of air forces participated in it—the Marine Corps with its helicopters and jets, the Army with its helicopters and transport aircraft, the Navy with its fighters, the Air Force with its bombers, transport aircraft, and fighters, and the South Vietnamese air force with its small number of fighters, helicopters, and transports. Retired Air Force General Richard Myers, who flew two tours as an F-4 pilot during the war, afterward lamented the lack of unity of command: "We had seven air forces working over there. Coordination between bombers and fighters was a rarity. Seventh Air Force, Thirteenth Air Force, the Navy, the Marines, bombers, and airlift all did their own thing. It wasn't as well coordinated as it could've—and should've—been."[16]

Much to the chagrin of Air Force leaders, operational control of B-52s in South Vietnam transferred from the Joint Chiefs in Washington, DC, to the commander of U.S. Pacific Command, Admiral Ulysses S. Grant Sharp, Jr., in Hawaii, and finally to Army General William Westmoreland, America's in-theater commander, who used the giant bombers as flying artillery to support ground forces. Air Force Chief of Staff General John McConnell believed that B-52s were inappropriate for Vietnam but nevertheless supported their continued employment there, "since the Air Force had pushed for the use of airpower to prevent Westmoreland from trying to fight the war solely with ground troops and helicopters."[17] The twisted parochialism and absence of centralized control diminished the prospects that the "airpower means" could make worthwhile contributions to obtaining the desired end of a stable, independent, noncommunist South Vietnam. Instead, such deficiencies significantly increased the likelihood that the aerial means—especially its kinetic component—would work against achieving that positive end. America's subsequent positive goal in the war would prove easier to achieve with airpower, but that was because the negative objectives changed as well, along with the character of the war itself.

Nixon's Use of Airpower in Vietnam

Despite the high-sounding tone of "peace with honor," President Nixon's positive goal in Vietnam was far more circumscribed, and he relied heavily on airpower to help him create a decent interval for the South's development and to recover American prisoners of war. Soon after taking office in 1969, he decided that bombing was the proper means to curtail the buildup of enemy forces in Cambodia, but since Cambodia was technically a neutral country, he would have to conduct the raids secretly. The raids continued unabated until May 1970, when the *New York Times* reported on the covert missions that had escaped the knowledge of both the Air Force Secretary and the Chief of Staff.[18] The duplicity suited Nixon with his moniker, "Tricky Dick," given that he had run for President on the platform of ending the war and now was enlarging it, albeit at the request of Cambodian Premier Norodom Sihanouk.[19]

The war that Nixon inherited, though, was not the same as the one fought by his predecessor. The 1968 Tet Offensive had decimated the VC as a significant fighting force and had also severely impaired the fighting capability of the NVA. Airpower had played a key role in the damage inflicted, with the bombing around the Marine base at Khe Sanh destroying two NVA divisions. Because of the losses suffered, the NVA again reverted to infrequent guerrilla warfare. When it returned to open combat with the "Easter Offensive" at the end of March 1972, it attacked with a fury resembling the World War II German blitzkrieg, minus the air support. More than 100,000 troops, supported by Soviet-supplied T-54 tanks and 130mm heavy artillery, attacked in a three-pronged assault against primarily South Vietnamese forces. (Nixon had by then removed most American troops from the war.[20]) The fast-paced, conventional character of the offensive, with its heavy requirements for fuel and ordnance, made it ideal for air attack, and the now-vital logistical resupply lines and bridges running back through North Vietnam became prime targets that finally paid dividends. Nixon ordered Air Force and Navy aircraft to pound the supply lines relentlessly in Operation *Linebacker*. He also mined the port of Haiphong. American aircraft further provided massive doses of close air support and logistical resupply to South Vietnamese forces that gradually stiffened their resistance.

Nixon could apply liberal amounts of airpower against targets in North Vietnam because he, unlike Johnson, had few negative political goals. Nixon and his savvy National Security Advisor Henry Kissinger, who often acted as Secretary of Defense and Secretary of State as well, had accurately gauged the growing animosity between China and the Soviet Union and decided to make it a centerpiece of their strategy of détente. A key price for securing the promise of diplomatic recognition to China and a strategic arms limitations treaty—and a wheat deal—with the Soviet Union was a free hand in dealing with North Vietnam. To Hanoi's dismay, both China and the Soviet Union ultimately provided Nixon with that freedom.[21] Nixon also had no equivalent of the "Great Society" to restrain his actions, and he believed that his success in establishing détente with the Chinese and Soviets would only enhance his—and America's—image on the world stage.

Nixon's profound concern for his image—and belief in his own infallibility—often spurred impromptu actions that had dire consequences for his air commanders. Before the North Vietnamese launched the Easter Offensive, evidence of the buildup for it caused Nixon to order a series of air strikes into North Vietnam in late December 1971. Then, in a February 3, 1972, Oval Office meeting with Kissinger and U.S. Ambassador to South Vietnam Ellsworth Bunker, Nixon increased the bombing. The President directed Bunker to notify Army General Creighton Abrams, who had replaced Westmoreland as theater commander in Vietnam, that Abrams could now attack surface-to-air missile (SAM) sites in North Vietnam, given that the North Vietnamese had begun firing SAMs at B-52s.[22] Air Force General John D. Lavelle, the commander of Seventh Air Force in Saigon, was responsible for carrying out the President's order. Lavelle's efforts to accomplish it merit close scrutiny, for they reveal the disastrous impact that presidential ego and complex ROE can have on commanders charged with implementing a desired air strategy.

For Lavelle, the ROE for air attacks against North Vietnam had changed significantly since President Johnson ended *Rolling Thunder* in October 1968. According to an agreement afterward, seemingly accepted by the North Vietnamese delegation at the Paris Peace Talks, American reconnaissance aircraft could fly over the North but no bombing would occur, provided the North Vietnamese did not engage in hostile actions against those aircraft.[23] Air Force fighters typically escorted those missions in case the North Vietnamese displayed hostile intent. If the pilots received fire or a headset warning tone indicating that a SAM radar was tracking their aircraft, they could respond with a "protective reaction strike."[24] In late 1971, the North Vietnamese "netted" their radar systems to allow ground-controlled interception radars to provide extensive information to SAM sites that minimized the need for SAM radar tracking, thereby minimizing—or eliminating—the warning tone pilots received prior to missile launch.[25]

General Lavelle determined that this move automatically demonstrated hostile intent from the North Vietnamese because by merely tracking an American aircraft with any radar, they could now fire at it with SAMs. For him, this blanket radar activation was sufficient for his pilots to fire on North Vietnamese SAM sites, though he was highly selective in the sites targeted. He received an endorsement of this perspective from Secretary of Defense Melvin Laird when Laird visited Saigon in December 1971. The Secretary told Lavelle to "make a liberal interpretation of the rules of engagement in the field and not come to Washington and ask him, under the political climate, to come out with an interpretation. I should make them in the field," Lavelle recalled, "and he would back me up."[26] Kissinger also wanted more intensified bombing, arguing for large raids on SAM sites in one fell swoop rather than attacks across several days that

U.S. Air Force Boeing B-52F Stratofortress from 320th Bomb Wing dropping bombs over Vietnam in mid-1960s (U.S. Air Force)

grabbed sustained attention in the media. The National Security Advisor told Admiral Thomas Moorer, the Chairman of the Joint Chiefs of Staff, “Our experience has been that you get the same amount of heat domestically for a four plane attack as you do for 400.”[27]

At the meeting with Kissinger and Ambassador Bunker on February 3, 1972, Nixon revealed that his understanding of ROE did not exactly match that of Laird and Lavelle, but the President’s intent was the same. Nixon declared that against SAMs, “protective reaction strikes” would now become “preventive reaction strikes” and that no one would know if SAMs had been fired at American aircraft first or not. He elaborated, “I am simply saying that we expand the definition of protective reaction to mean preventive reaction where a SAM site is concerned. . . . Who the hell’s gonna say they didn’t fire?” The President added, “Do it, but don’t say anything. . . . He [Abrams] can hit SAM sites period.”[28]

Nixon’s directive reached Lavelle, who then began an assault on SAM sites in the southern panhandle of North Vietnam. Nixon requested to be kept apprised of air attacks on all North Vietnamese targets and received a detailed, daily compilation of the missions. Those reports originated from Lavelle and were in turn passed up the chain of command, with Admiral Moorer, Secretary Laird, and Kissinger reviewing them before they went to the President. On no occasion did Nixon express displeasure with the bombing; in contrast, on the February 8 report, he scribbled a note in the margin for Kissinger: “K—is there *anything* Abrams has asked for that I have *not* approved?”[29]

Lavelle’s actions did not, however, receive universal endorsement. Lonnie Franks, an Air Force technical sergeant who recorded mission results for computer compilation in Saigon, was baffled when pilots erroneously reported enemy ground fire as the rationale for bombing Northern targets. Lavelle had told subordinates that they could not report “no enemy reaction” after raids, but he had failed to explain that any North Vietnamese radar activation constituted a hostile act that justified a bombing response. The form that Franks used to record data contained only four reasons for expending

Flying under radar control with B-66 Destroyer, Air Force F-105 Thunderchief pilots bomb North Vietnam military target, June 14, 1966 (U.S. Air Force/NARA/Cecil J. Poss)

ordnance over North Vietnam: fire from antiaircraft artillery, MiGs, SAMs, or small arms—no block existed for "radar activation." Pilots thus chose one of the listed options, and Franks, knowing that the selections were incorrect, thought that the effort to deceive was deliberate and wrote his Senator. An Inspector General investigation ensued and Lavelle was removed from command and demoted to major general following hearings by the House and Senate Armed Services committees.

When Nixon heard of Lavelle's dismissal, the President expressed remorse that the general had been sacked for conducting missions that Nixon had ordered. "I just don't want him to be made a goat, goddammit," Nixon said to Kissinger in June 1972. Kissinger responded, "What happened with Lavelle was he had reason to believe that we wanted him to take aggressive steps," to which Nixon replied, "Right, that's right." The President then stated, "I don't want a man persecuted for doing what he thought was right. I just don't want it done." He then disparaged Sergeant Franks, comparing him to Daniel Ellsberg, who had leaked the *Pentagon Papers.* Kissinger replied, "Of course, the military are impossible, too," to which Nixon responded, "Well, they all turn on each other like rats." Kissinger offered, "I think that this will go away. I think we should just say a . . . after all we took corrective steps. We could have easily hidden it. I think you might as well make a virtue of necessity." To that, Nixon responded, "I don't like to have the feeling that the military can get out of control. Well, maybe this censures that. This says we do something when they, . . ." and he stopped in mid-sentence. Then he added, "It's just a hell of a damn. And it's a bad rap for him, Henry."[30]

A week later, Nixon decided to take Kissinger's advice. In a June 22 news conference, the President answered questions about Lavelle's dismissal by stating, "The Secretary of Defense has stated his view on that; he has made a decision on it. I think it was an appropriate decision."[31] Nixon further stated to the press a week later, "But he [Lavelle] did exceed authorization; it was proper for him to be relieved and retired. And I think it was the proper action to take, and I believe that will assure that kind of activity may not occur in the future."[32]

Lavelle became the highest-ranking American officer to receive a public rebuke for trying to implement his President's air strategy, but he was not the only air commander to suffer from Nixon's callousness and ego. Air Force General John W. Vogt, Jr., who replaced Lavelle, visited the White House on his way to Saigon and described Nixon as "wild-eyed" as he berated commanders for lacking aggressiveness in attacking the Easter Offensive. "He wanted somebody to use imagination—like Patton," Vogt remembered.[33] The President elaborated on those thoughts to Kissinger in a memorandum soon after the *Linebacker* campaign had begun:

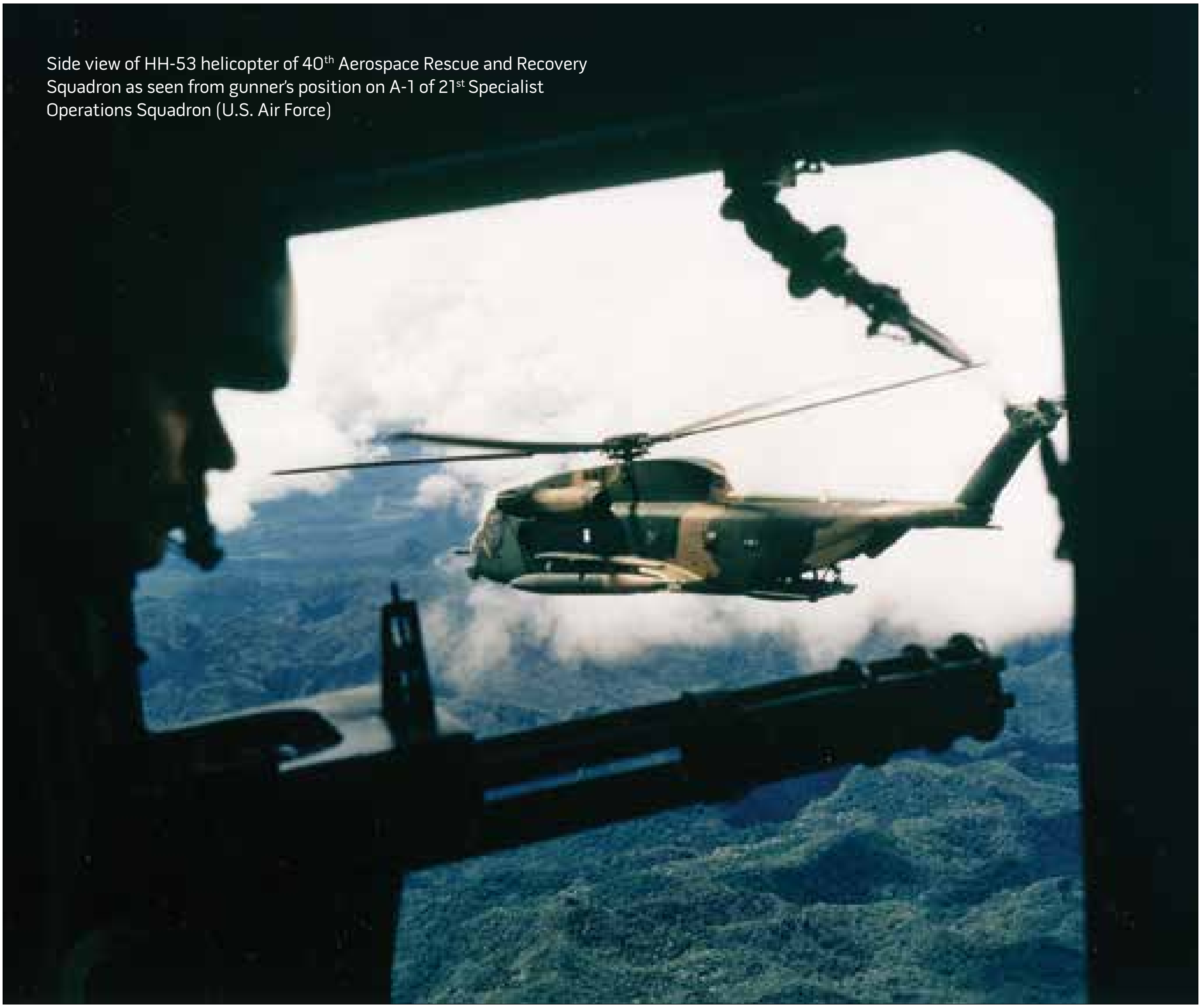
> *I want you to convey directly to the Air Force that I am thoroughly disgusted with their performance in North Vietnam. Their refusal to fly unless the ceiling is 4,000 feet or more is without doubt one of the most pusillanimous attitudes we have ever had in the whole fine history of the U.S. military. I do not blame the fine Air Force pilots who do a fantastic job in so many other areas. I do blame the commanders who, because they have been playing "how not to lose" for so long, now can't bring themselves to start playing "how to win." Under the circumstances, I have decided to take command of all strikes in North Vietnam in the Hanoi-Haiphong area out from under any Air Force jurisdiction whatever. The orders will be given directly from a Naval commander whom I will select. If there is one more instance of whining about target restrictions we will simply blow the whistle on this whole sorry performance of our Air Force in failing for day after day after day in North Vietnam this past week to hit enormously important targets when they had an opportunity to do so and were ordered to do so and then wouldn't carry out the order.*[34]

Nixon never followed through on his threat to eliminate Air Force commanders from the air war against North Vietnam, but he continued to berate military leaders as they worked to implement his increasingly effective air strategy. That strategy proved successful partly because the North Vietnamese persisted in waging conventional war. As long as they did so, their troop concentrations in the South were vulnerable to aerial assault, as were their vital supply lines. The strategy was also successful because the positive ends that Nixon sought from it were extremely limited. Besides securing the return of American POWs, he aimed for an agreement assuring South Vietnam's survival for a brief period of time, and personally guaranteed to South Vietnamese President Nguyen Van Thieu that the South would not fall while he was in office.[35] Accordingly, Nixon had Kissinger propose an "in-place cease-fire" to Northern negotiators in Paris, which spurred NVA efforts to secure additional territory despite the aerial pounding they sustained. The North Vietnamese responded to Nixon's offer by dropping their demand for Thieu to resign, and a peace accord appeared imminent in late October 1972 when the President ended *Linebacker*. Neither Nixon nor Kissinger had informed Thieu of the in-place cease-fire offer, however, and once Thieu learned of it, he was incensed.

Thieu's refusal to accept the tentative Paris settlement led to a breakdown in the peace talks and caused Nixon to return to his "airpower means" to secure his positive ends—which now included convincing Thieu that he could depend on Nixon's promise of future military backing. In addition, the President now had a negative political objective that would constrain the amount of force that he could apply. Although he had won a resounding reelection victory in early November, the Democrats seized control of both houses of Congress and threatened to terminate spending for the war when Congress convened in early January. With limited time available to achieve results, Nixon decided to turn to the B-52, with its enormous 30-ton bomb load, to do the job. The President had already shifted more than half of the Strategic Air Command (SAC) fleet of 400 heavy bombers to air bases in Guam and Thailand. He thought that risking the B-52—a vital component of America's nuclear triad—in raids against targets in the well-defended Northern heartland would demonstrate just how serious his efforts were to end the war. On December 14, in Washington, Nixon gave the order for bombing to begin 3 days later—December 18 in Vietnam. In customary fashion, he told Admiral Thomas H. Moorer, the Chairman of the Joint Chiefs of Staff, "I don't want any more crap about the fact that we couldn't hit this target or that one. This is your chance to use military power effectively to win this war and if you don't I'll consider you personally responsible."[36]

For the crews of more than 200 B-52s, the operation dubbed *Linebacker II* marked the first time that any of them had flown against targets in Hanoi; the bombers had raided Haiphong targets only once before, in April 1972. Still, as the influx of bombers in the Pacific had steadily increased, Air Force General J.C. Meyer, the SAC commander, anticipated such an operation and ordered Lieutenant General Gerald Johnson, the commander of Eighth Air Force, on Guam, to design a plan for it. Johnson and his staff submitted the desired plan to Meyer in November 1972.[37] Yet when Nixon's order to begin the assault arrived at SAC headquarters, Meyer chose to disregard the Eighth Air Force plan, and had his own staff in Omaha, Nebraska, create one instead.

The short timespan to produce a plan led to a design with minimal ingenuity. Aircraft used the same flight paths to attack targets at the same times for the first 3 nights. The North Vietnamese took advantage of the repetitive routing to mass their SAM batteries in the areas where the B-52s turned off target and then fired their SAMs ballistically, which negated the bombers' defensive capabilities. The initial 3 nights produced the loss of eight bombers, with five more heavily damaged; another two fell to SAMs on the night of December 21. Meyer ended the repetitive routing and, after a 36-hour stand-down for Christmas, turned over planning for the remainder of the operation to Eighth Air Force.



Side view of HH-53 helicopter of 40th Aerospace Rescue and Recovery Squadron as seen from gunner's position on A-1 of 21st Specialist Operations Squadron (U.S. Air Force)

On December 26, General Johnson's staff implemented the plan they had designed, with 120 B-52s attacking targets in Hanoi and Haiphong from nine different directions in a 15-minute timespan. Two bombers fell to SAMs (a loss rate of 1.66 percent), and the next day, in Washington, Nixon received word that the North Vietnamese were ready to resume negotiations in Paris on January 8. The President responded that negotiations had to begin on January 2 and would have a time limit attached, and that the North Vietnamese could not deliberate on agreements already made.[38] On December 28, Hanoi accepted Nixon's conditions, and he ended *Linebacker II* the next day. In 11 days, the North Vietnamese downed 15 bombers, but in doing so exhausted most of their supply of SAMs. The mercurial Nixon credited the Air Force with success, telling aide Chuck Colson, "The North Vietnamese have agreed to go back to the negotiating table on our terms. They can't take bombing any longer. Our Air Force really did the job."[39] The President continued bombing North Vietnam south of the 20th parallel until the initialing of the Paris Peace Accords on January 23, 1973.

For many air commanders, Nixon's dramatic "Christmas Bombing" vindicated their belief that airpower could have won the war had President Johnson employed a comparable operation in spring 1965.[40] Nixon himself made a similar assertion in April 1988 when he appeared on *Meet the Press* and stated that his greatest mistake as President was not Watergate but the failure to conduct *Linebacker II* in 1969 after he took office. "If we had done that then," he said, "I think we would have ended the war in 1969 rather than 1973."[41] Such assertions demonstrate that the Commander in Chief—as well as many military leaders—never really understood that the character of the war in 1972 had changed dramatically from what it had been for most of the conflict. The change to conventional warfare with the Easter Offensive was a key reason why airpower yielded tangible results.

Moreover, the success that Nixon achieved with airpower stemmed from his pursuit of positive and negative political objectives that differed significantly from those of his predecessor. Nixon had no illusions about pursuing a stable, independent, noncommunist South Vietnam; the shock of the 1968 Tet Offensive turned American public opinion against the war and made leaving Vietnam the new positive goal. Although he labeled that objective "peace with honor," in the end Nixon accepted a settlement that offered South Vietnam a possibility of survival, not a guarantee. He gave South Vietnamese President Thieu an ultimatum to accept that agreement, noting that without Thieu's approval the U.S. Congress would likely cut off all funding to South Vietnam. Whether *Linebacker II* persuaded Thieu that he could count on Nixon for support after the signing of the Paris Peace Accords remains a matter for conjecture; the agreement that Thieu reluctantly endorsed in January 1973 differed little from what Kissinger had negotiated in October 1972.

Nixon's lack of negative political goals enabled him to apply airpower more aggressively than Johnson. With no conflicting loyalties to a domestic agenda like Johnson, and with détente effectively removing China and the Soviet Union from the equation, Nixon had mainly to worry about the compressed time that Congress gave him to achieve a settlement. Nixon knew that his image would suffer because of the intensified bombing and was willing to accept that tarnishing, though he did not condone indiscriminate attacks. The 20,000 tons of bombs dropped in *Linebacker II* killed 1,623 civilians, according to North Vietnamese figures—an incredibly low total for the tonnage dropped.[42] Yet in all likelihood, the comparatively unrestrained, nonstop aerial pounding that the NVA received in South Vietnam counted as much, if not more, than Nixon's focused bombing of the North. The attacks in the South directly threatened the NVA's survival, and without that force on Southern soil, the North faced a more difficult path conquering South Vietnam.[43] Ultimately, airpower helped to assure that a flawed South Vietnamese government lasted for a few more years.

Legacies of Airpower in Vietnam

In the final analysis, several legacies emerged from airpower's ordeal in Vietnam. The dismal lack of unity of command displayed there spurred development of the joint force air component commander concept, in which a single air commander directs the flying activities of multiple Services to achieve objectives sought by the joint force commander. In terms of Air Force doctrine, *Linebacker II*'s perceived success in compelling the North Vietnamese to negotiate reinforced the belief that airpower could achieve political goals cheaply and efficiently. The 1984 edition of the Air Force's *Basic Doctrine Manual* noted:

> *unless offensive action is initiated, military victory is seldom possible. . . . Aerospace forces possess a capability to seize the offensive and can be employed rapidly and directly against enemy targets. Aerospace forces have the power to penetrate to the heart of an enemy's strength without first defeating defending forces in detail.*[44]

The manual further encouraged air commanders to conduct strategic attacks against "heartland targets" that would "produce benefits beyond the proportion of effort expended and costs involved," but cautioned that such attacks could "be limited by overriding political concerns, the intensity of enemy defenses, or more pressing needs on the battlefield."[45]

The impact of such "overriding political concerns" on the application of airpower is a key legacy of the air wars in Vietnam. To commanders who had fought as junior officers in World War II, where virtually no negative objectives limited military force, the tight controls that President Johnson placed on bombing North Vietnam chafed those charged with wielding the air weapon. Navy Admiral U.S. Grant Sharp, who directed *Rolling Thunder* as the commander of U.S. Pacific Command, wrote in the preface of his 1977 memoir *Strategy for Defeat*:

> *Our airpower did not fail us; it was the decision makers. And if I am unsurprisingly critical of those decision makers, I offer no apology. My conscience and my professional record both stand clear. Just as I believe unequivocally that the civilian authority is supreme under our Constitution, so I hold it reasonable that, once committed, the political leadership should seek and, in the main, heed the advice of military professionals in the conduct of military operations.*[46]

Many American Airmen from the war likely agreed with Sharp's critique.

Operation *Rolling Thunder* highlighted how negative political objectives could limit an air campaign. Indeed, in the American air offensives waged since Vietnam—to include the use of unmanned aerial vehicles against "high-value" terrorist targets—negative goals have continued to constrain the use of military force. Projecting a sound image while applying airpower was difficult enough for American leaders in Vietnam; today's leaders must contend with 24/7 news coverage as well as social media accounts that enable virtually anyone to spin a story and reach a large audience. In the limited wars that the Nation will fight, negative objectives will always be present, and those objectives will produce ROE that limit airpower. "War is always going to have restrictions—it's never going to be [Curtis] LeMay saying 'Just bomb them,'" stated General Myers, the most recent Air Force Chairman of the Joint Chiefs of Staff.[47] Against insurgent enemies, the negative objectives may well eclipse the positive goals sought. When that occurs, kinetic airpower's ability to yield success will be uncertain.

Yet because airpower, as a subset of war, is not only a political instrument but also one that is applied by humans, it will be subject to the whims and frailties of the political leader who chooses to rely on it. Richard Nixon saw himself as a Patton-esque figure who could swiftly and efficiently brandish military force to achieve his aims. He felt little compunction in berating his air commanders or—in the case of General Lavelle—casting one adrift when he

Two U.S. Navy Douglas A-7B Corsair II from attack squadron VA-25 during 1969 Ironhand mission over North Vietnam (U.S. Navy)

thought that doing so might save him embarrassment. Nixon believed that airpower gave him the ideal military tool for threatening an opponent or persuading an ally, and that perspective has gained traction since he left the White House. The last four occupants of the Oval Office, to include President Barack Obama, have all relied heavily on airpower in the conflicts they have fought. The positive goals pursued—"stability," "security," and, on occasion, "democracy"—have proved difficult to achieve with any military force, particularly with airpower. Its siren song is an enticing one, however, as Johns Hopkins Professor Eliot Cohen has astutely observed, "Airpower is an unusually seductive form of military strength, in part because, like modern courtship, it appears to offer gratification without commitment."[48] That promise is a dangerous one, as General Myers warns:

> *The last thing that we want is for the political leadership to think war is too easy, especially in terms of casualties. It's awful; it's horrible, but sometimes it's necessary.* [The decision for war] *needs to be taken with thoughtful solemnness—with the realization that innocent people, along with combatants, will get hurt.*[49]

Were he alive today, the Prussian military philosopher Carl von Clausewitz would doubtless nod in agreement at General Myers's observation.

But Clausewitz never saw an airplane; if he had, though, his airpower notions would likely have been unsurprising. Had he examined America's air wars in Vietnam, he would certainly have commented about the difficulty of achieving political objectives in a limited war. In all probability, he would have looked at President Johnson's Tuesday lunch–targeting process, the Route Package system dividing North Vietnamese airspace, the creation of free fire zones in the South, Nixon's condemnation of his air commanders and dismissal of General Lavelle, the repetitive B-52 routing for *Linebacker II*, and any number of other elements of the U.S. experience in Vietnam and stated simply: "Friction rules." "Everything in strategy is very simple," Clausewitz wrote, "but that does not mean that everything is very easy."[50] Perhaps the most enduring legacy of the air wars in Vietnam is the one that applies to *any* military strategy—uncertainty, chance, danger, and stress will be certain to limit it. JFQ

This article was originally presented as a lecture at the Royal Australian Air Force's airpower conference in Canberra, Australia, March 2014, and appears as a chapter in the conference proceedings *A Century of Military Aviation 1914–2014*, edited by Keith Brent (RAAF Air Power Development Centre, 2015).

Notes

[1] Raphael Littauer and Norman Uphoff, eds., *The Air War in Indochina* (Boston: Beacon Press, 1972), 11, 168–172; and Earl H. Tilford, Jr., *Crosswinds: The Air Force's Setup in Vietnam* (College Station: Texas A&M University Press, 1993), 109.

[2] *U.S. Foreign Policy for the 1970s: Shaping a Durable Peace—A Report to the Congress by Richard Nixon, President of the United States, May 3, 1973* (Washington, DC: U.S. Government Printing Office, 1973), 59. Nixon commented about the Paris Peace Agreement: "While our essential principles were met, we and the Communists had to make compromises. Many of these were more significant for our ally than for us. . . . Our friends have every opportunity to demonstrate their inherent strength." Two months earlier the President had told Alexander Haig: "The country would care if South Vietnam became Communist in a matter of six months. They would not give a damn if it's in two years." See Tape Subject Log, Conversation 416-43, Nixon Presidential Library and Museum, March 17, 1973 (hereafter, Nixon Presidential Library).

[3] Doris Kearns Goodwin, *Lyndon Johnson and the American Dream* (New York: Signet, 1976), 263.

[4] "Meeting with Foreign Policy Advisors on Vietnam," August 18, 1967, Meeting Notes File, Box 1, Lyndon Baines Johnson Presidential Library (hereafter, Johnson Library); Headquarters U.S. Air Force, *Analysis of Effectiveness of Interdiction in Southeast Asia, Second Progress Report*, May 1966, Air Force Historical Research Agency (hereafter, AFHRA), file K168.187-21, 7. Robert McNamara acknowledged in 1967 that communist forces fought an average of 1 day in 30 and that they needed 15 tons of supplies daily from external sources. The Joint Chiefs of Staff had estimated in August 1965 that the enemy needed 13 tons per day of "external logistical support." See U.S. Congress, Senate, Committee on Armed

Services, Preparedness Investigating Subcommittee, *Air War against North Vietnam*, 90th Cong., 1st sess., August 25, 1967, pt. 4, 299; and Annex A to JCSM 613-65, August 27, 1965, National Security Files (hereafter, NSF), Country File: Vietnam, Folder 2 EE, Box 75, Johnson Library. The standard military 2½-ton truck could transport 5 tons of goods over roads and 2½ tons overland. Regarding North Vietnam's import capacity, see Walt Rostow to the President, May 6, 1967, NSF, Country File: Vietnam, Folder 2EE, Box 75, Johnson Library; and *The Pentagon Papers: The Defense Department History of United States Decisionmaking on Vietnam*, *The Senator Gravel Edition*, 5 vols. (Boston: Beacon Press, 1971), 4: 146.

[5] Guenter Lewy, *America in Vietnam* (New York: Oxford University Press, 1978), 309.

[6] Stanley Karnow, *Vietnam: A History* (New York: Penguin Books, 1997), 455–456, 672, 675.

[7] National Security Action Memorandum 328, April 6, 1965, NSF, Boxes 1–9, Johnson Library.

[8] Memorandum, McNamara for the President, July 28, 1965, NSF, National Security Council History, "Deployment of Major U.S. Forces to Vietnam, July 1965," Vol. 1, Box 40, Johnson Library.

[9] David C. Humphrey, "Tuesday Lunch at the Johnson White House: A Preliminary Assessment," *Diplomatic History* 8 (Winter 1984), 90.

[10] U.S. Air Force Oral History interview of Major General Robert N. Ginsburgh by Colonel John E. Van Duyn and Major Richard B. Clement, May 26, 1971, AFHRA, file K239.0512-477, 65–68; and interview of Lieutenant Colonel William H. Greenhalgh by the author, Maxwell Air Force Base, May 17, 1985.

[11] U.S. Air Force Oral History interview of Lieutenant General Joseph H. Moore by Major Samuel E. Riddlebarger and Lieutenant Colonel Valentino Castellina, November 22, 1969, AFHRA, file K239.0512-241, 17–18.

[12] Robert L. Gallucci, *Neither Peace nor Honor: The Politics of American Military Policy in Viet-Nam* (Baltimore: The Johns Hopkins University Press, 1975), 80–84; Littauer and Uphoff, 38. In July 1966, after a span of poor weather obscured targets over the North, Seventh Air Force Commander General William C. Momyer ordered his fighter pilots not to fly and called for ground crews to perform preventive maintenance on the aircraft. A message then arrived from the Pentagon telling Momyer to fly to prevent the Navy from achieving a higher sortie count. See Greenhalgh interview, May 17, 1985.

[13] Interview by the author of a Navy A-4 pilot who wished to remain anonymous.

[14] Air Force Colonel Jack Broughton, a veteran F-105 pilot, called North Vietnam "the center of hell with Hanoi as its hub." See Jack Broughton, *Thud Ridge* (New York: Bantam Books, 1969), 24.

[15] Free fire zones were "known enemy strongholds . . . virtually uninhabited by noncombatants" where any identified activity was presumed to stem from enemy forces and was thus susceptible to immediate air or artillery strikes. See Sean A. Kelleher, "Free Fire Zones," in *Dictionary of the Vietnam War*, ed. James S. Olson (Westport: Greenwood, 1988), 163.

[16] Interview of General Richard Myers by the author, National Defense University, November 26, 2013.

[17] John Schlight, *The United States Air Force in Southeast Asia: The War in South Vietnam: The Years of the Offensive 1965–1968* (Washington, DC: Office of Air Force History, 1988), 82.

[18] Earl H. Tilford, Jr., *Setup: What the Air Force Did and Why in Vietnam* (Maxwell Air Force Base, AL: Air University Press, 1991), 196. The secret bombing deposited 120,578 tons of bombs on Cambodian soil. See Carl Berger, ed., *The United States Air Force in Southeast Asia, 1961–1973: An Illustrated Account* (Washington, DC: Office of Air Force History, 1984), 141.

[19] Tilford, 194; and Richard Nixon, *RN: The Memoirs of Richard Nixon*, 2 vols. (New York: Warner Books, 1978), 1: 472.

[20] By May 1972, only 69,000 American troops remained in Vietnam, and most of them were not in combat units.

[21] Hanoi's communist party newspaper *Nhan Dan* described China and the Soviet Union's policy of détente as "throwing a life-

U.S. Air Force F-5 aircraft refueling from KC-135 tanker before bombing Viet Cong position (U.S. Air Force photo) buoy to a drowning pirate . . . in order to serve one's narrow national interests." See *Nhan Dan* editorial, August 17, 1972, in Gareth Porter, ed., *Vietnam: The Definitive Documentation of Human Decisions*, 2 vols. (Stanfordville, NY: Earl M. Coleman, 1979), 2: 568.

[22] "Conversation Among President Nixon, the President's Assistant for National Security Affairs (Kissinger), and the Ambassador to South Vietnam (Bunker)," Washington, DC, February 3, 1972, in *Foreign Relations of the United States, 1969–1976, Vol. VIII: Vietnam, January–October 1972* (Washington, DC: U.S. Government Printing Office, 2010), 71–78.

[23] In addition to agreeing not to fire on American reconnaissance aircraft in return for a bombing halt, North Vietnamese negotiators also seemingly agreed that their forces would not move men and supplies across the DMZ or fire on major South Vietnamese cities. President Johnson was convinced that North Vietnamese subscribed to the "agreement." He wrote in his memoirs: "Before I made my decision [to halt the bombing], I wanted to be absolutely certain that Hanoi understood our position. . . . Our negotiators reported that the North Vietnamese would give no flat guarantees; that was in keeping with their stand that the bombing had to be stopped without conditions. But they had told us if we stopped the bombing, they would 'know what to do.' [American negotiators] were confident Hanoi knew precisely what we meant and would avoid the actions that we had warned them would imperil a bombing halt." Lyndon Baines Johnson, *The Vantage Point: Perspectives of the Presidency, 1963–1969* (New York: Holt, Rinehart & Winston, 1971), 518.

[24] Aloysius Casey and Patrick Casey, "Lavelle, Nixon, and the White House Tapes," *Air Force Magazine*, February 2007, 87.

[25] Ibid.

[26] Quoted in ibid. In a 2007 letter to the editor of *Air Force Magazine*, Melvin Laird stated, "It was certainly true that in my meetings with Gen. John Lavelle I told him that my order on 'protective reaction' should be viewed liberally. . . . Prior to my order, there was no authorization (under McNamara or [Secretary of Defense Clark] Clifford) to destroy dangerous targets except when fired upon without special permission. Gen. Bus Wheeler [Moorer's predecessor as Chairman of the Joint Chiefs of Staff], Adm. Tom Moorer, and Gen Abrams all agreed with the liberal interpretation on my order on protective reaction. The new orders permitted hitting anti-aircraft installations and other dangerous targets if spotted on their missions, whether they were activated or not." See Melvin R. Laird, "Letter to the Editor," *Air Force Magazine*, May 2007, 4.

[27] "Minutes of a Senior Review Group Meeting, Subject: Vietnam Assessment," Washington, DC, January 24, 1972, *Foreign Relations of the United States, 1969–1976, Vol. VIII* (Washington, DC: U.S. Government Printing Office, 2010), 25.

[28] "Conversation Among President Nixon et al.," 74–75.

[29] "Memorandum for the President from Henry A. Kissinger, Subject: Secretary Laird's Daily Report on Southeast Asia Situation," February 8, 1972; Folder: Vietnam, January–February 1972 (2 of 3); Box 158, National Security Council Files, Nixon Presidential Library. Emphasis in original.

[30] "Meeting between Henry Kissinger and the President," June 14, 1972, Oval Office, WHT Reference Cassette, C-2240 RC-2, 733-6, Nixon Presidential Library.

[31] "Transcript of the President's News Conference Emphasizing Domestic Matters," *New York Times*, June 23, 1972.

[32] "Transcript of President Nixon's News Conference Emphasizing Foreign Affairs," New York Times, June 30, 1972.

[33] Quoted in Seymour M. Hersh, *The Price of Power: Kissinger in the Nixon White House* (New York: Summit Books, 1983), 506.

[34] "Memorandum for Henry Kissinger and Al Haig from the President," May 19, 1972, White House Special Files, Staff Member and Office Files, President's Personal File, Box 4, "Memo—May 1972," Nixon Presidential Library. Emphasis in original.

[35] Nixon expressed this commitment to Thieu in a letter dated January 5, 1973, and sent Alexander Haig to Saigon in the middle of the month to convey the President's commitment personally. See Nixon, *RN, 2:* 245–246; and Henry A. Kissinger, *White House Years* (Boston: Little, Brown, 1979), 1459–1462, 1469. Yet in forthright conversation with Kissinger during an intense phase of the Paris negotiations, Nixon confessed, "Let's be perfectly cold-blooded about it. If you look at it from the standpoint of our game with the Soviets and the Chinese, from the standpoint of running this country, I think we could take, in my view, almost anything, frankly, that we can force on Thieu. Almost anything. I just come down to that. You know what I mean? Because I have a feeling we would not be doing, like I feel about the Israeli[s], I feel that in the long run we're probably not doing them an in—uh . . . a disfavor due to the fact that I feel that the North Vietnamese are so badly hurt that the South Vietnamese are probably going to do fairly well. But also due to the fact—because I look at the tide of history out there, South Vietnam is never going to survive anyway. I'm just being perfectly candid." The conversation continued, with Kissinger concluding, "So we've got to find some formula that holds the thing together for a year or two, after which—after a year, Mr. President, Vietnam will be a backwater. If we settle it, say, this October, by January '74 no one will give a damn." See "Conversation between President Richard Nixon and Henry Kissinger," Conversation 760-6, August 3, 1972, Richard Nixon Presidential Materials Project, NARA, Presidential Recordings Program, Miller Center of Public Affairs, University of Virginia, available at <http://whitehousetapes.net/clips/1972_0803_vietnam/index.htm>.

[36] Nixon, *RN, 2:* 242.

[37] Interview of Colonel Clyde E. Bodenheimer by the author, January 7, 1983, Maxwell Air Force Base.

[38] Kissinger, *White House Years*, 1457–1458; and Nixon, RN, 2: 250.

[39] Charles W. Colson, *Born Again* (Grand Rapids, MI: Chosen Books, 1976), 78.

[40] See, for example, "What Admiral Moorer Really Said About Airpower's Effectiveness in SEA," *Air Force Magazine*, November 1973, 25; Howard Silber, "SAC Chief: B-52s Devastated Viet Air Defenses," *Omaha World Herald*, February 25, 1973; U.S. Air Force Oral History Interview of Lieutenant General Gerald W. Johnson by Charles K. Hopkins, April 3, 1973, Andersen Air Force Base, Guam, AFHRA, file K239.0512-831, 11–13; U.S. Air Force Oral History Interview of General John W. Vogt by Lieutenant Colonel Arthur W. McCants, Jr., and Dr. James C. Hasdorff, August 8–9, 1978, AFHRA, file K239.0512-1093, 69; U.S. Grant Sharp, *Strategy for Defeat: Vietnam in Retrospect* (San Rafael, CA: Presidio Press, 1978), 252, 255, 272; and William W. Momyer, *Airpower in Three Wars* (Washington, DC: U.S. Government Printing Office, 1978), 339.

[41] Richard M. Nixon, statement on NBC's *Meet the Press*, April 10, 1988.

[42] Murray Marder, "North Vietnam: Taking Pride in Punishment," *Washington Post*, February 4, 1973.

[43] Observed General Tran Van Tra, commander of communist forces in the southern half of South Vietnam, after having undergone 9 months of continual bombing: "Our cadres and men were fatigued, we had not had time to make up for our losses, all units were in disarray, there was a lack of manpower, and there were shortages of food and ammunition. . . . The troops were no longer capable of fighting." Tran Van Tra, *Concluding the 30-Years War* (Ho Chi Minh City, 1982 [in Vietnamese]; reprint ed. [in English], Arlington, VA: Joint Publications Research Service, 1983), 33; quoted in Gabriel Kolko, *Anatomy of a War: Vietnam, the United States, and the Modern Historical Experience* (New York: Pantheon Books, 1985), 444–445.

[44] Air Force Manual 1-1, *Basic Aerospace Doctrine of the United States Air Force* (Washington, DC: Headquarters U.S. Air Force, March 16, 1984), 2–6.

[45] Ibid., 2–12.

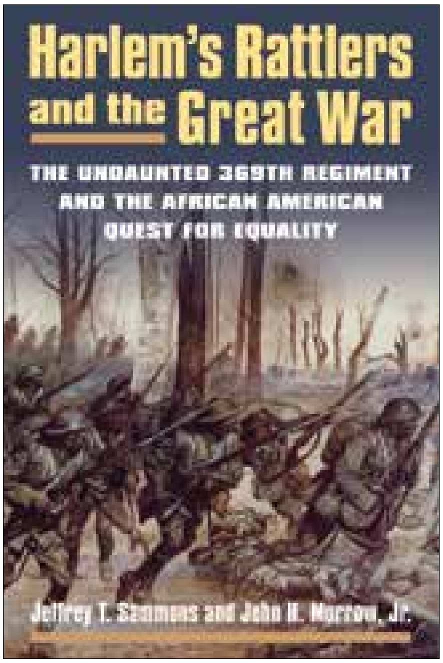
[46] Sharp, xvii.

[47] Myers interview, November 26, 2013.

[48] Eliot A. Cohen, "The Mystique of U.S. Airpower," *Foreign Affairs* 73 (January–February 1994), 109.

[49] Myers interview, November 26, 2013.

[50] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 178.


Harlem's Rattlers and the Great War
THE UNDAUNTED 369TH REGIMENT AND THE AFRICAN AMERICAN QUEST FOR EQUALITY
Jeffrey T. Sammons and John H. Morrow, Jr.

Harlem's Rattlers and the Great War: The Undaunted 369th Regiment and the African American Quest for Equality

By Jeffrey T. Sammons and John H. Morrow, Jr.
University Press of Kansas, 2014
616 pp. $34.95
ISBN: 978-0700619573

Reviewed by Alan L. Gropman

In 1903, W.E.B. Du Bois, the eminent American sociologist, scholar, and leader, wrote that "the problem of the twentieth century is the problem of the color-line." Recent events in Ferguson, Missouri; Staten Island, New York; Cleveland, Ohio; and North Charleston, South Carolina should make us realize that, despite America's recent racial progress, the problem of the 21st century is still the color-line. *Harlem's Rattlers* lays bare the bigotry that African-American citizens faced in the early 20th century and, more importantly, details the innumerable accomplishments by black American soldiers despite the racism propagated by the President of the United States, U.S. military, and bigoted American civilians.

This book is the definitive history of the 369th Regiment in World War I, an outstanding black infantry regiment comprised of 3,000 men led by a white command element. It is the most complete, scholarly, and fully documented account of this famous (and underpublicized) unit, unlikely to be superseded. The authors, both prominent historians, are renowned experts in their fields.

Sammons and Morrow tell the complete story of the 369th—a combat unit that grew out of the 15th New York National Guard Regiment—from the bigotry that black leaders initially had to overcome to create the unit and the herculean efforts required to convince both New York city and state politicians hostile to the idea of an all-black unit to their valiant service in France and their ultimately humiliating return to the United States after having spent more time in the trenches that any other U.S. combat unit. The book also examines the postwar tribulations of the 369th and contains several epilogues that detail the unit's combat losses, postwar histories of the key officers and men, and unfortunate lives of two of the unit's most famous warriors: Henry Johnson, who, nearly 100 years after the war's end, is under consideration to receive the Congressional Medal of Honor, and Neadom Roberts.

Why the title *Harlem's Rattlers*? That was what the men called themselves—not "Men of Bronze" or "Harlem's Hellfighters," terms often used incorrectly in other histories of the unit. The men of the 369th thought of the rattlesnake as a symbol of power (like the Gadsden flag used during the Revolutionary War that depicted a coiled snake atop the words "Don't Tread on Me!"). This and many of the other myths associated with the 369th are rewritten by the authors, bringing truthfulness and clarity to a story that has long been riddled with inaccuracies.

The authors devote approximately one-fifth of the book to describing the domestic political issues within both the New York state and the federal governments, as well as the turbulent conflict within the black community, over the formation of an all-black combat unit. Once formed, training for the 15th New York National Guard Regiment was difficult for a number of reasons, most of them racial.

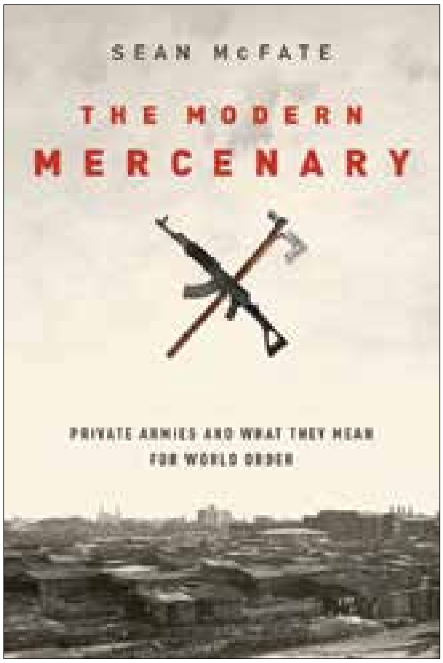
Black political and social leaders including W.E.B. Du Bois thought there was a positive correlation between serving as uniformed soldiers and possessing full citizenship. Why they believed they could improve the situation of black Americans through military service is difficult to understand. A dearth of both recognition and reward defined the service of black soldiers during the Civil War, in which nearly 40,000 died, the Indian Wars, in which they comprised a far greater proportion of the Army than they did the U.S. population in general, and the Spanish-American War, during which all four historic black regiments fought. These black leaders struggled continually to convince the War Department and U.S. Government to establish black infantry units and to permit blacks to serve in combat. Even men as sophisticated as Du Bois, however, underestimated the depth of bigotry in the country; there would be no rewards for the black soldiers for their service in World War I. In fact, following the end of the conflict, political and social conditions for black civilians were worse than they had been prior to its outbreak.

Training for the 369th was to have been completed in Spartanburg, South Carolina, prior to the soldiers' departure for the frontlines in France. Racist treatment of the soldiers by the city's inhabitants, however, nearly provoked an armed attack on Spartanburg by the unit, forcing the War Department to send the 369th overseas without having been fully trained. Once in France, the American Expeditionary Force commanders did not want to attach the 369th to any U.S. division and instead assigned them to a French division. The performance of the 369th in combat was distinguished, and the men of the unit were highly praised by their French commanders for their determination, cohesion, high morale, and fighting capability. Despite this, when the U.S. Army Chief of Staff asked the Army War College in 1924 to make recommendations regarding future racial policy, the authors of the study disregarded the heroism of the 369th and produced a document that was blatant in its racism.

The chief was advised to maintain racial segregation and to ensure that all-black fighting units were commanded by whites. The study concluded, incorrectly, that blacks believed themselves to be inferior to whites and that they were "by nature" subservient, lacking "initiative and resourcefulness" because, as stated in the report, "[t]he cranial cavity of the Negro is smaller than the white; his brain weighs 35 ounces contrasted with 45 for the white." Most damning, however, was the illogical argument that "[i]n physical courage . . . the American Negro falls well back of the white man and possibly behind all other races." This statement flew in the face of the numerous black soldiers who had served with honor in the Civil War, Indians Wars, and Spanish-American War and were awarded congressional medals of honor in recognition of their courage and valor. (No medals of honor were awarded during the 20th century for World War I.) The report was prepared by the entire student body and faculty at the Army War College in 1924 and 1925 with nine additional iterations appearing prior to the start of World War II; the same racist notions were included in each report. The United States in general—and the U.S. Army in particular—paid a steep price for allowing the country's deeply entrenched racism to define—and limit—the use of a courageous, determined, and highly capable fighting force in World War II.

Harlem's Rattlers is a soundly researched and documented history that all Americans—and especially military officers—should read. **JFQ**

Dr. Alan L. Gropman is Professor Emeritus in the Dwight D. Eisenhower School for National Security and Resources Strategy at the National Defense University.



The Modern Mercenary: Private Armies and What They Mean for World Order

By Sean McFate
Oxford University Press, 2014
235 pp. $29.95
ISBN: 978-0199360109

Reviewed by T.X. Hammes

At their peak, contractors comprised more than 50 percent of U.S. personnel in Iraq and Afghanistan. Furthermore, despite complaints about contractor performance, the Pentagon has stated that contractors will make up half of any future U.S. force deployments. Why? Because they work. This reality requires defense professionals to seek a deeper understanding of what contractors do and the implications for future conflict—making Sean McFate's *The Modern Mercenary* a very timely book. In it, he not only carefully examines contractors, but also describes the changing international environment in which they will operate.

McFate does not claim his book covers all aspects of contracting. Rather, he focuses on the most controversial element: private military companies or, in his words, "the private sector equivalent of combat arms." As he notes, the most disturbing aspect of the Pentagon's increasing reliance on contractors is "the decision to outsource lethal force." He places these companies in two categories. Those that directly apply military force are "mercenaries," while those that train others to do so are "enterprisers." These categories represent two distinct markets. Mercenaries exist as a free market in which each individual sells his or her services directly to the buyer, offering the means of war to anyone who can afford it. Enterprisers represent a mediated market in which the company is an arbitrator between the individual and the buyer. Essentially, the company recruits and organizes personnel to fulfill specific mission/contract requirements as defined by the buyer. For good business reasons, enterprisers are more discriminating in both the clients and tasks they accept. Unfortunately, if business demands, enterprisers can easily slip to the mercenary side of the scale.

McFate does not see mercenaries and enterprisers in the same light. Using Somalia as a case study, he argues that free market mercenaries are likely to contribute to increased instability and will not improve a state's chances of success. In contrast, enterprisers offer a state an opportunity for success. He uses Liberia as a case study where, as a DynCorp employee, he participated in raising and training the new Liberian army. However, his argument for enterprisers is weakened by the lack of success in Iraq and Afghanistan despite the presence of dozens, if not hundreds, of enterprisers.

In one of the most interesting aspects of this intriguing work, McFate applies the concept of neo-medievalism—the belief that the world is becoming increasingly non–state-centric and multipolar—to describe the emerging global security environment. While states will remain major players, overlapping authorities and allegiances will have major impacts on how and why wars are fought and who fights them.

In this environment, McFate states, "the private military industry has a bright future. This multi-billion-dollar industry will not simply evaporate once the United States withdraws from overseas deployments such as Afghanistan. In fact, the opposite will occur: contractors will help fill the security vacuum left by US forces. . . . Already, private military companies of all stripes are seeking new opportunities in conflict zones in Africa, the Middle East, and Latin America." He notes four trends that are driving this global expansion. First, private companies are resilient and strive to grow. They will be assisted in that growth by the next two trends: globalization and indigenization. Globalization is driving military contracting to seek overseas markets. At the same time, the numerous third country nationals who were hired by U.S. firms in Iraq and Afghanistan will take their new business and technical skills home and indigenize the market. Finally, the market will bifurcate into two major categories: mediated and free-market segments.

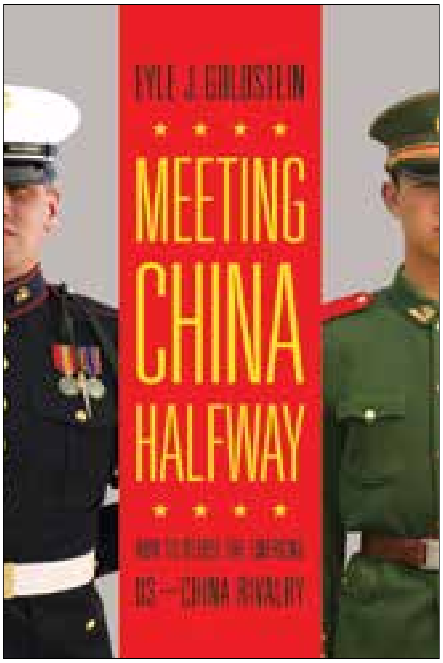
McFate's meticulously researched and well-presented work concludes that "private military actors worsen security in a free market such as Somalia but increase it in a mediated market such as Liberia and under the right market conditions could even prove a powerful tool for the United Nations and others." This reviewer found McFate's two categories useful, but they understate the complexities of modern military contracting. The reader must understand that McFate is really describing a spectrum from pure individual mercenary to major corporate enterpriser.

McFate concludes by cautioning that the:

> *United States has limited regulation of and oversight over the private military industry despite employing it widely. This creates opportunities for abuse by contactors as firms subtly steer client decisions in favor of profit over policy goals, altering strategic outcomes in the process. The objectives of [private military companies] and their clients will differ, just as those of the condottieri and the provveditori did in the Middle Ages.*

If he is right about the growth of military contracting—and current Defense Department policy indicates he is—any U.S. forces deployed overseas must expect to work with, and perhaps fight against, armed contractors. It is a subject that requires our professional attention, and *The Modern Mercenary* is a great place to start. JFQ

Dr. T.X. Hammes is a Distinguished Research Fellow in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.



Meeting China Halfway: How to Defuse the Emerging U.S.-China Rivalry

By Lyle J. Goldstein
Georgetown University Press, 2015
400 pp. $29.95
ISBN: 978-1626161603

Reviewed by Christopher Nelson

China is on the minds of many today. In fact, an informal term has been coined for the group of scholars and defense officials who spend most of their waking hours thinking, talking, and writing about China. They are so-called China Watchers. In no other foreign policy realm is a similar term used with such frequency. This alone should give everyone pause. Watching for what, exactly?

With "watchers" there comes readers. There is an unending stream of books and magazine articles on China. Of course, this is both frustrating and promising. It is frustrating because there are too many books to choose from; many of us simply do not have the time to read, let alone to think about many of these issues. It is promising because with more minds turned to the challenges and opportunities of a rising China, statistically one hopes, good ideas and solutions will surface.

Policy books on China generally fall into one of two categories. First, there is the realist camp, which is occupied by authors and officials who believe the United States should engage China on issues of mutual concern (for example, humanitarian assistance/disaster relief and antipiracy operations), yet at the same time ensure the U.S. military, particularly the U.S. Navy, is prepared, armed, and equipped to defeat Chinese aggression if necessary. At the heart of the realist opinion is the belief that humanity is inherently competitive and nonbenevolent and that conciliatory gestures will only weaken one's national security. Aaron Friedberg's book *The Contest for Supremacy* falls somewhere in this description. The second type of policy book comes from the liberal internationalism crowd. This view stresses that problems are better resolved in an international forum: a system composed of states in which diplomacy reigns supreme and where bargains and compromise are the ultimate goals. Hugh White's book *The China Choice: Why We Should Share Power* fits this description.

Lyle J. Goldstein, then, in his ambitious new book *Meeting China Halfway* continues where White leaves off. Goldstein, a professor at the Chinese Maritime Studies Institute at the U.S. Naval War College, and a fluent Chinese speaker and reader, takes White's argument for sharing power with China and expands on it, arguing that the United States needs to develop "cooperation spirals." With these spirals, Goldstein asserts, "trust and confidence are built over time through incremental and reciprocal steps that gradually lead to larger and more significant compromises." Goldstein then proceeds to take a host of issues that concern the United States and China—Taiwan, the economy, the environment, the developing world, the Persian Spring, the Korean Peninsula, Southeast Asia, and finally, India—and then applies a cooperation spiral to each. This adds up to a healthy amount of policy prescriptions. By the end of the book Goldstein has provided, for the United States alone, at least 50 policy recommendations tied to cooperation spirals.

Take, for example, the current U.S.-China hot topic issue: the South China Sea. In the chapter titled "The New 'Fulda Gap,'" Goldstein acknowledges that the South China Sea is the region with the "greatest arena of contention." He then offers 10 policy recommendations—5 for the U.S. and 5 for China—to stabilize the region. He begins with the United States allowing the Chinese to participate in Cooperation Afloat Readiness and Training exercises. Following this, the Chinese could propose a joint counterpiracy patrol in the Strait of Malacca. Next, the United States should propose a Southeast Asia coast guard forum, and then the Chinese should open the Hainan naval complex to visits from the Association of Southeast Asian Nations. Goldstein also recommends that the United States should reduce its surveillance flights in parts of the South China Sea, and then China should clarify its island claims. Finally, he works his way up to the last of 10 policy prescriptions: the Chinese should end their military cooperation with the Philippines and Indonesia, and the United States should then end its military cooperation with Vietnam. His book illustrates this back-and-forth quite nicely by using a graphic in each chapter showing the cooperation spiral using arrows and text in English and in Chinese.

Goldstein anticipates the criticism that his book will generate. Namely he knows that there are plenty of critics who will label his idea of cooperation spirals appeasement. These critics, of course, are coming from the more hawkish corners of the U.S. Government, including the military. Yet a more pressing criticism is that if U.S. and Chinese interests are so opposed then any conciliatory efforts are meaningless. Even if China and the United States accepted some provisions of Goldstein's cooperation spiral, this would not ensure greater security; it would only mean that both nations have found some common ground on issues that are at the periphery. The crux of the matter still remains: The United States desires a region that behaves and abides by one set of rules, but China, on the other hand, desires a region that abides by another.

Goldstein has written a book that is ambitious and is one of few China policy books arguing for a conciliatory way forward in this tense and possibly deadly game of brinksmanship. Regardless if you agree with Goldstein's arguments or prescriptions, any China Watcher will get something out of his close reading of Chinese and English policy and military documents. To his credit, Goldstein notes that there are voices in China that are not monolithic and xenophobic. To believe in an inevitable fight between the United States and China is fatalistic. Rather, one should read Goldstein's work with both an open mind and healthy skepticism. JFQ

Lieutenant Commander Christopher Nelson, USN, is an Intelligence Officer and recent graduate of the U.S. Naval War College and Maritime Advanced Warfighting School.

U.S. Air Force F-22 Raptor aircraft after conducting airstrikes in Syria as part of large coalition to strike Islamic State of Iraq and the Levant targets, September 2014 (DOD/Jefferson S. Heiland)

Three Approaches to Center of Gravity Analysis

The Islamic State of Iraq and the Levant

By Daniel J. Smith, Kelley Jeter, and Odin Westgaard

Since the establishment of the center of gravity (COG) concept as a fundamental planning factor in joint military doctrine, its proper identification has been considered crucial in successful attainment of desired objectives. Joint Publication 5-0, *Joint Operation Planning*, states, "This process cannot be taken lightly, since a faulty conclusion resulting from a poor or hasty analysis can have very serious consequences, such as the inability to achieve strategic and operational objectives at an acceptable cost."[1]

Since its inception as a core planning tenet, the process for determining COGs has been a point of contention and debate. Currently, the definition of *center of gravity* and the process for determining it are outlined in joint doctrine, specifically in Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, JP 3-0, *Joint Operations*, and JP 5-0, *Joint Operation Planning*, as encompassed in the Joint Operation Planning Process (JOPP) within those publications. Speculation on proper COG determination has given rise to other COG methodologies, which have both questioned and challenged established doctrine for COG determination. Therefore, the objective of this article is to compare and contrast different COG determination methodologies to reveal strengths and weaknesses of each and ultimately to make recommendations for changes to joint doctrine. To accomplish this objective, three different COG methodologies are applied to the current Islamic State of Iraq and the Levant (ISIL)[2] problem set: Dale C. Eikmeier's COG determination method, James P. Butler's Godzilla COG methodology, and the Critical Factors Analysis, outlined in the JOPP.[3] Findings of the analyses will be critically compared to produce recommendations for changes in joint doctrine COG determination.

When ISIL initiated large-scale offensive operations into Iraq in early June 2014, it propelled itself onto the global stage. While other contemporary Islamic militant groups have stated similar objectives for establishing an Islamic caliphate,[4] ISIL is unique in that it has made significant progress in pursuit of that goal by seizing control of large amounts of territory in Iraq and Syria. With manning estimated at around 20,000 to 31,500,[5] ISIL has been forcefully seizing territory in a conventional military fashion (while still sometimes employing contemporary insurgency-type tactics). In doing so, ISIL has been acquiring more supplies and sources of revenue to fuel its operations. The following COG methodologies will not only explicate each one's structured processes, but also reveal other essential variables in detail.

The Eikmeier COG Methodology

Joint Publication 5-0 defines *center of gravity* as "a source of power that provides moral or physical strength, freedom of action, or will to act."[6] Eikmeier's proposed COG definition states that "the center of gravity is the primary entity that possesses the inherent capability to achieve the objective."[7] With this COG specificity, Eikmeier's method is comprised of six steps:[8]

- Identify the desired ends or objectives.
- Identify the ways to achieve the ends, and select the one that evidence suggests is most likely to work. (Ways are actions, so they are expressed as verbs.) Then select the most elemental or essential action—that selection is the critical capability. The ways are critical actions that will achieve the endstate. Critical capabilities (CC) are the same verbs expressed in the ways; therefore, ways equal critical capabilities.
- List the means (critical requirements) needed to enable and execute the ways (critical capabilities).
- Select from the list of means the entity (noun) that possesses the innate way (CC) to tangibly achieve the end. This selection is the center of gravity.
- From the remaining items on the list, select those that are critical for the execution of the critical capability, which are the critical requirements.
- Complete the process by identifying those critical requirements vulnerable to adversary actions.

Once these steps are complete, the results of the COG analysis must pass the "does/uses" test; that is, the center of gravity is the means (critical requirement) that has the intrinsic force necessary, which "does" the action (critical capability), but it "uses" or requires other resources (means) to "do" the action. An example is the game of football. (For simplicity's sake, the example focuses only on offense.)

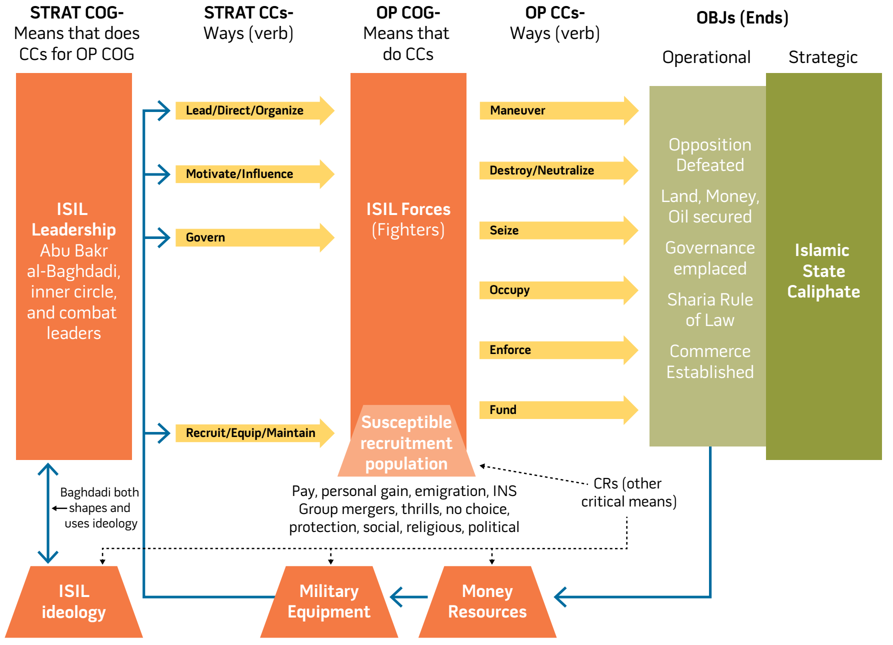
- Step one: identify ends. The grand strategic objective is to win a championship. Other strategic objectives are winning games or winning a division. Operational objectives are to score touchdowns. Tactical objectives are scoring first downs.
- Step two: the ways (critical capabilities) to achieve the endstate, which are expressed as verbs. Strategically, they would include *assembling* a winning team, *recruiting/retaining* the right players, *emplacing/substituting* the right players, *calling* the right plays, and *making* the right calls. Strategically, the types of offense that coaches *employ* and their *decisionmaking* both determine operationally who will *run, pass/catch, block, kick,* and so forth.
- Step three: means (critical requirements) required to accomplish the ways. Strategically, coaches and their supporting staffs are the means necessary to manage, organize, train, and supply a football team. Operationally, the means are, but are not limited to, adequate equipment, practices, physical training facilities, morale, and the players themselves.
- Step four: entity (noun) from the list of means that intrinsically possesses the capabilities to achieve the ends. From the list, only the players can *run, pass, catch*, and *execute* plays—they are the operational COG. The coaches possess the inherent capability to decide which players will *play* (*run, pass,* and so forth); therefore, they are the strategic COG.
- Step five: critical requirements essential for the centers of gravity to reach the ends. These include recruiting, player placement, practices, fitness facilities/programs, and morale. While these requirements are essential, they are not centers of gravity. Coaches choose/insert players, and players win games.

Now that we understand this methodology, we apply it to determine ISIL's center of gravity (figure 1).

Step One: Identifying ISIL's Ends. The group's identified strategic objective

Major Daniel J. Smith, USA, is a Strategic Intelligence Officer currently serving as the Ground Force Analysis Manager with the Technology Long-Range Analysis Division at the Defense Intelligence Agency. Major Kelley Jeter, USAF, currently serves as a Public Affairs Officer at the Headquarters U.S. Air Force press desk. Master Gunnery Sergeant Odin Westgaard, USMC, currently serves as a Sustainment Observer/Trainer in the Joint Staff J7.

Figure 1.



since 2014 has been the establishment of an Islamic caliphate in which it possesses authority over Muslims worldwide and aims to bring most Muslim-inhabited regions of the world under its political control, beginning with the Levant region, which generally includes Syria, Jordan, Israel, Palestine, Lebanon, Cyprus, and part of southern Turkey.[9] On June 29, 2014, ISIL declared the establishment of a caliphate. Its current leader, Abu Bakr al-Baghdadi, who has renamed himself Amir al-Mu'minin Caliph Ibrahim, was named as caliph.[10]

To accomplish this strategic objective, the following operational objectives must be successfully completed: Opposition in Syria and Iraq (military and civilian) must be neutralized or destroyed.[11] Land must be seized and secured within Syria and Iraq.[12] Governance must be established in conquered areas.[13] Sharia law must be established in conquered territory (this is implied as a caliphate requirement). Adequate revenue to establish sufficient commerce for governance and funding must be gained and maintained (with oil as the main resource).[14]

Step Two: Ways (CCs) Necessary for ISIL to Accomplish Objectives.

- *Maneuver* to conduct offensive operations
- *destroy/neutralize* opposition
- ability to *seize* territory
- ability to *occupy* seized lands
- *enforce* sharia law
- *govern* provinces, cities, and territory
- *fund* operations and new governance
- *lead, direct,* and *organize* ISIL
- *motivate* and *influence* ISIL *recruit* and *maintain* capable forces.[15]

Step Three: Means or Critical Requirements Necessary to Execute Ways (Critical Capabilities).

- Adequate fighter strength: ISIL fighters are estimated to number around 20,000–31,500.[16]
- Military equipment: ISIL has attained large amounts of assault rifles, machine guns, rocket-propelled grenades, surface-to-air missiles, other antiarmor weapons, artillery, tanks, light vehicles, armored personnel carriers, antiaircraft weaponry, and various other rocket-launcher systems.[17]
- Leadership and leadership structure: ISIL has a clear leader with a well-structured cabinet and subordinate leadership. Abu Bakr al-Baghdadi is the declared caliph, and he has a cabinet of advisors that includes two deputy leaders, one for Iraq and one for Syria. There are also 12 local governors with supporting staffs.[18]
- Fighter morale/will to fight: Islamic ideology is one morale factor that ISIL leadership uses for recruitment and for exploiting common demographics and psychosociological factors found in many members of terrorist organizations.[19] However, ISIL leadership also lures recruits with pay/housing incentives and protection. Some recruits are thrill-seekers, while some join only for personal gain. Smaller insurgent groups join ISIL as a merger of convenience. Tribes that have surrendered to ISIL are often compelled to join the organization or face the threat of severe consequences.[20]
- Funding: ISIL funds itself through the seizure of assets in conquered territory, the sale of oil on the black market, extortion, and external support.[21]

Step Four: Entities That Possess Distinctive Ways to Achieve Operational and Strategic Ends. These selections are the respective centers of gravity. The critical requirement that possesses the capability to accomplish the identified objectives is the ISIL fighters themselves; therefore, this army is ISIL's operational center of gravity. However, it took significant effort to mobilize the ISIL army. ISIL leadership "does" the work of *recruiting, organizing, governing,* and continually *motivating* ISIL fighters and "uses" them to *maneuver, defeat, seize, occupy,* and *enforce* as necessary for ISIL to accomplish its objectives. Therefore, Abu Bakr al-Baghdadi and his inner circle are the strategic center of gravity.

Two U.S. Air Force F-15E Strike Eagle aircraft fly over northern Iraq after conducting airstrikes against ISIL targets in Syria (DOD/Matthew Bruch)

Step Five: Further Validates COG Selection. From the remaining items on the critical requirement list that are vital for the execution of the critical capabilities, the fighters "do" the operational work by "using" the other critical requirements necessary, which were mostly seized by the fighters in the first place. The fighters themselves seized more weapons and equipment for use and did not attain enhanced capabilities as a result of prior government issuing. Furthermore, although ISIL has gained greater capabilities, its fighters—infantrymen—are ISIL's core strength. Military equipment, money, and other resources cannot be employed, seized, or exploited without ISIL fighters.

ISIL leadership "does" the work to create, maintain, and lead its army, and "uses" this army to accomplish its objectives. If ISIL were already a state actor with an established government, military, and economy, its current leadership would not qualify as the strategic center of gravity, according to Eikmeier.[22] However, ISIL is not a state actor. Abu Bakr al-Baghdadi took the helm of the moderately effective Islamic State in Iraq in 2010 and developed it into the formidable force that it is today.[23] As a kingdom requires a king, a caliphate requires a caliph, and al-Baghdadi established himself as the first caliph. It is one thing to need or employ an existing force; it is another thing to *create* it first. If ISIL becomes more firmly established and continues to be successful, the strategic center of gravity likely will shift toward its revenue sources. Removing a key leader from a securely established entity probably would not cause it to collapse, as a new leader would move in to take his place; however, as of now, ISIL is still a nascent organization that requires astute leadership to hold it together.[24]

The process concludes by identifying those critical requirements vulnerable to adversary actions. As the ISIL fighters are the operational COG, various factors contribute to the filling of ISIL's fighter ranks. The mergers of convenience (personal/group survival and protection) indicate that if more ideal options became available, fighters might consider renouncing ISIL. Disruption in revenue could hinder incentives to fight for ISIL, inciting reconsiderations of convictions.[25] Events such as these could also potentially increase friction and distrust in leadership. Exploitation of these vulnerabilities could significantly damage ISIL's centers of gravity.

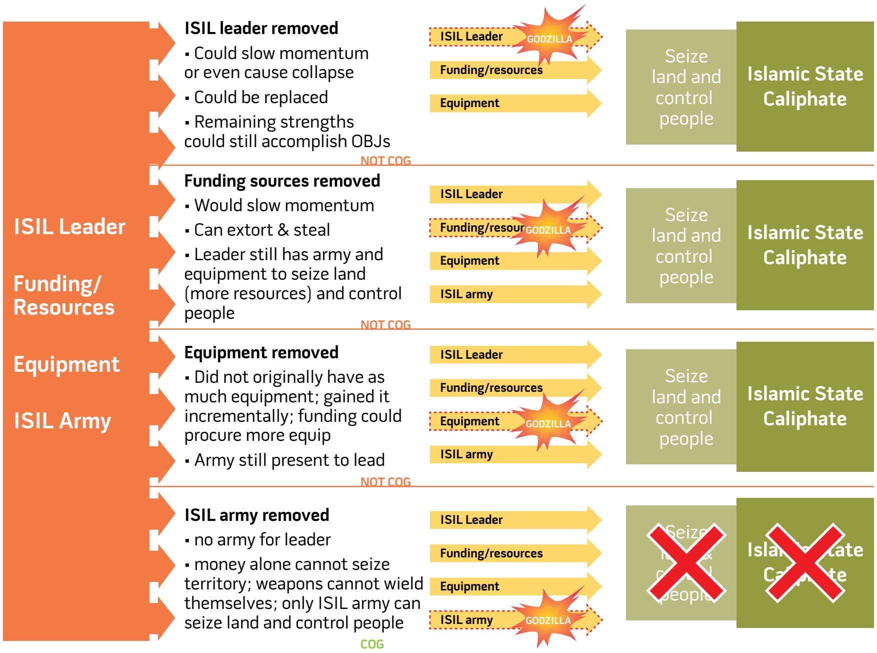
Eikmeier's COG determination methodology provides tangible centers of gravity, which are determined through a testable "does/uses" criteria. For the operational COG, identification of this criterion is a more objective process than with identification of the strategic COG, but it is still testable under the criteria. If the methodology is followed correctly, COG identification likely would be more consistent with its results, regardless of who applies the technique.

Godzilla COG Methodology

Another alternative methodology that possesses testable criteria is Butler's Godzilla COG determination approach. The Godzilla methodology is relatively simple. Butler essentially determines the overall strategic goal of the force to be examined—friendly or enemy—and examines the objective that must be met to achieve that goal. Once the operational objective has been determined, the critical strengths for achieving that objective are identified. Next, these strengths are removed and examined one at a time. The Godzilla methodology posits that one of these critical strengths is the center of gravity. To identify that center, as a critical strength is removed, the question then asked is: can the objective still be achieved without this strength? If the answer is yes, that strength is not the center of gravity. The strength is replaced and another is removed, asking the same question. Once we find the sole strength—the removal of which precludes the accomplishment of the objective—the center of gravity has been identified (see figure 2).[26]

Figure 2.

Center of Gravity Candidates (Identified Critical Strengths)


ISIL Leader
Funding/ Resources
Equipment
ISIL Army
ISIL leader removed
• Could slow momentum or even cause collapse
• Could be replaced
• Remaining strengths could still accomplish OBJs
NOT COG
Funding sources removed
• Would slow momentum
• Can extort & steal
• Leader still has army and equipment to seize land (more resources) and control people
NOT COG
Equipment removed
• Did not originally have as much equipment; gained it incrementally; funding could procure more equip
• Army still present to lead
NOT COG
ISIL army removed
• no army for leader
• money alone cannot seize territory; weapons cannot wield themselves; only ISIL army can seize land and control people
COG
ISIL Leader
Funding/resources
Equipment
ISIL army
GODZILLA
Seize land and control people
Islamic State Caliphate

ISIL leader, funding, and equipment are certainly critical strengths, but these strengths are applied to ensure ISIL has a capable army to accomplish its objectives. The leader needs an army. Critical to amassing a capable army is adequate funding. Only its army can physically seize and control people—other strengths are enablers to this.

Just because the ISIL army is the COG as per the Godzilla method does not mean planning excludes focus on the other critical strengths. Contrarily, if unable to kinetically destroy the army, then focusing on some or all of the identified strengths may be the only way to dismantle the ISIL army.

Butler uses Milan Vego's definitions to best describe critical strengths as the "primary sources of physical or moral potential/power or elements that integrate, protect, and sustain specific sources of combat potential/power."[27] Strengths are therefore considered critical if they "affect or potentially affect achievement of the objective."[28]

To get to that point with ISIL, we must examine its stated strategic objective and means for achieving it. ISIL has declared an Islamic caliphate, and its strategic objective is to expand the borders and influence of that caliphate as far as possible, governing all its citizens under strict sharia law. With this as its stated strategic objective, what must ISIL accomplish to make this goal a reality?

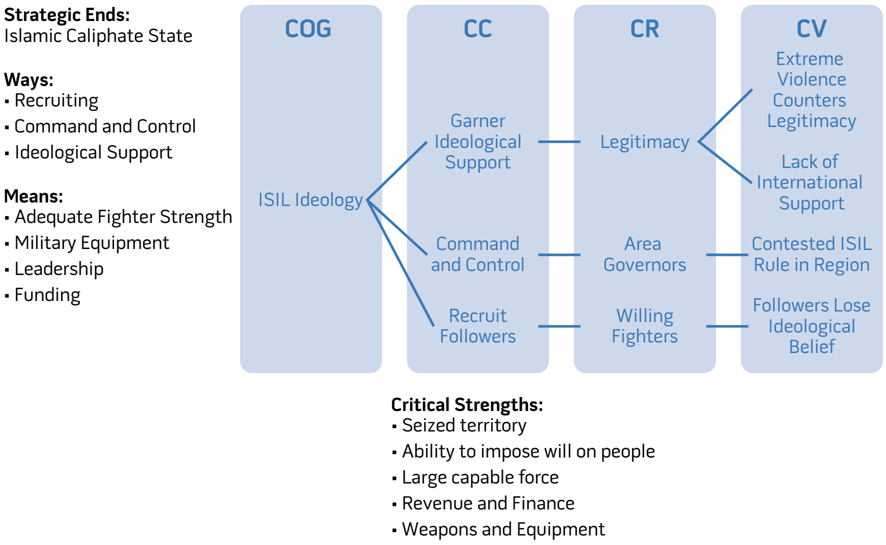
First and foremost, what ISIL has so far accomplished is what sets it apart from other Islamic extremist groups. It has seized land, controls a large population, and currently governs as the declared caliphate. Therefore, controlling land and people to spread its sphere of governance is the decisive operational objective that defines the caliphate. Accomplishing these advances has taken several critical strengths unique to ISIL: capable and charismatic leadership, an army of 20,000 to 31,500 armed members, large amounts of equipment, and highly lucrative funding sources. This army has been critical in seizing much of the previously mentioned equipment and revenue. Using the Godzilla methodology, these strengths are next removed one at a time to identify the indispensable strength that is the center of gravity.

Abu Bakr al-Baghdadi's leadership and will to expand territory and govern people are key elements that set ISIL apart from its contemporaries. Removing that leadership in the early days of the movement might have completely derailed its progress and dispersed its followers. But the momentum of the organization, as it currently is, has grown beyond just the influence of one man, and removing al-Baghdadi might even promote him to martyr status and galvanize his followers behind his replacement. The replacement might not be as effective a leader, but there is no guarantee that removing this strength would prevent ISIL from attaining its objectives. Therefore, it does not follow at this point that al-Baghdadi is the center of gravity.

The army ISIL has amassed is a motivated group that has obeyed the orders to seize territory and subjugate citizens throughout its territory in Iraq and Syria. They are well armed, trained, brutal, and, from all outward appearances, motivated and highly capable of conquering, holding, and governing the territories and people they are charged with dominating. ISIL is well armed largely because of the sizeable amounts of military hardware it has captured through progressive victories. Through these victories, ISIL also has seized valuable sources of revenue, notably oil fields, to continue funding its operations.

Large quantities of newly acquired weapons, while critical, cannot exclusively accomplish ISIL's objectives; someone must wield them. Impeding money and resources could prove critical in suppressing ISIL, but its fighters intrinsically retain the capability to seize territory, subjugate citizens, and hold territory. Removing these militants from the equation would render the leadership of ISIL relatively impotent. Declaring a caliphate will fall on deaf ears if the means for enforcing it and growing

Figure 3.


COG
CC
CR
CV
ISIL Ideology
Garner Ideological Support
Command and Control
Recruit Followers
Legitimacy
Area Governors
Willing Fighters
Extreme Violence Counters Legitimacy
Lack of International Support
Contested ISIL Rule in Region
Followers Lose Ideological Belief

Strategic Ends:
Islamic Caliphate State

Ways:
- Recruiting
- Command and Control
- Ideological Support

Means:
- Adequate Fighter Strength
- Military Equipment
- Leadership
- Funding

Critical Strengths:
- Seized territory
- Ability to impose will on people
- Large capable force
- Revenue and Finance
- Weapons and Equipment

it are taken away. Therefore, based on the COG identification criteria outlined by the Godzilla method, the substantial army that ISIL has amassed is its center of gravity.

Critical Factors Analysis COG Methodology

Now that nondoctrinal COG methodologies have been applied to the current ISIL problem set, the Critical Factors Analysis COG determination methodology outlined in the JOPP is applied to ISIL. Joint Publication 5-0 states that the first step in COG analysis is to identify the desired objectives.[29] Upon examination of ISIL from various open sources, its main strategic objective is to create an Islamic state across Sunni areas of Iraq and in Syria.[30] Al-Baghdadi is ISIL's self-declared leader and seeks authority over all Muslims.

Nested with this strategic objective, operational objectives are to control Sunni areas in Iraq, recruit more fighters, and continue to gain funding. As the JOPP COG methodology next outlines, critical strengths, critical weaknesses, centers of gravity, critical capabilities, critical requirements, and critical vulnerabilities must be identified. Finally, decisive points are identified (see figure 3). Below, these variables are outlined with the JOPP process.[31]

1a. Strategic Objective(s)
   a. creation of an Islamic State
   b. uniting all Muslims
   c. defeating U.S. and Western allies.

1b. Operational Objective(s)
   a. control of Sunni areas in Iraq and Syria
   b. recruit more fighters
   c. gain funding to support efforts.

2a. Critical Strengths
   a. large following of personnel willing to fight for the cause
   b. weapons seized from captured areas in Iraq and Syria
   c. financially gain from seized equipment, oil fields, and trafficking operations
   d. rule by terror to subjugate inhabitants.

2b. Critical Weakness(s)
   a. nonstate actor (seeking to become legitimized state)
   b. no international endorsement (further delegitimizes ISIL)
   c. rule by terror (could espouse uprising)
   d. radical followers' loyalty is tied to religious and ideological beliefs of leader.

3a. Strategic Center of Gravity: radical ISIL ideology.

3b. Operational Center of Gravity: ISIL forces.

4. Critical Capabilities
   a. ability to recruit followers
   b. ability to garner support for ideology
   c. command and control of forces across wide areas of terrain.[32]

5. Critical Requirements
   a. legitimacy
   b. sustainment
   c. fighters.

6. Critical Vulnerabilities
   a. no cohesive acceptance of Islamic ideology (that is, Sunni versus Shia) in disputed area
   b. extreme violence could reduce willingness of fighters.

7. Decisive Points
   a. control of towns and villages within Iraq and Syria
   b. terrorist activity is a backup to overt rule in Iraq and Syria and will contribute to overall objectives of ISIL.

Based on analysis of the identified critical factors, the conclusion we reach is that the ISIL movement appears reliant on the continuation of popular support for the radical Sunni ISIL ideology, that is, the strategic COG. If belief in the strategic COG followed by al-Baghdadi and his immediate supporters wavers, or if other Islamic ideological variants garner more support, the ISIL movement likely will fall apart.

Comparison Findings

Eikmeier's COG application identified ISIL leadership as the strategic center of gravity, with the ISIL fighters as the operational center of gravity. The Godzilla methodology determined that the ISIL fighters are the COG. The JOPP method identified the ISIL ideology as the strategic COG, with the ISIL fighters as the operational COG. As evident, all three methods yielded similar results for the ISIL fighters as a COG, with differences in the identification of the strategic COG. With the Eikmeier application, the ISIL ideology is identified as a critical requirement (means) that its leadership shapes and uses to recruit, motivate, and influence ISIL fighters to accomplish its objectives. Leadership in this JOPP application is not specifically identified as a critical factor but is inherently implied within other outlined critical factors; it is also implied as necessary in the JOPP method conclusion statement.

For argument's sake, whether identified as a COG or a critical requirement, understanding all variables that contribute to the effectiveness of ISIL ideology in recruiting and motivating is essential if planning is focused on countering the ideology. To plan operations centered on the neutralization of an ideology means to focus on the people it is influencing. In addition to the ISIL recruitment base described earlier, much research conducted on ideology-driven terrorist organizations indicates that most terrorists are social solidarity seekers. They search for social acceptance, with a majority of members being poor, unmarried, rejected socially, or dislocated from their native lands.[33] Recent studies on al Qaeda, Fatah, Hamas, Hezbollah, Palestinian Islamic Jihad, and Turkish terrorists have revealed that a key reason for joining was that a friend or relative was already a member, a conclusion consistent with prior research on many other terrorist groups.[34] Much terrorism research tends to gravitate toward ideological causation but fails to address consistent socioeconomic and demographic variables that are prevalent within terrorist organizations. ISIL is no exception to this phenomenon.

The COGs identified with the JOPP method are not testable under this process. As different people apply the JOPP process, varying results are inevitable and often become subject to debate. All three methods provide structured processes for identifying critical COG variables. Objectives (ends), critical capabilities (ways), critical requirements (means), and other critical variables are inherent in all three methods. The primary difference is that the Eikmeier and Godzilla applications provide testable criteria for COG determination, whereas the JOPP process lacks a definitive COG qualifying procedure, making it more subjective in nature and thus more susceptible to biases, preferences, or dominant personalities.

Then-Secretary Hagel and General Dempsey testify before Senate Armed Services Committee regarding President Obama's authorized military strikes in Syria to destroy, degrade, and defeat ISIL (DOD/Daniel Hinton)

With the analyses and findings of these methodologies, current joint doctrine for center of gravity determination should be revised. A new methodology does not necessarily need to directly mirror Eikmeier's or Butler's COG methodologies, but it does need to make joint doctrine COG determination a testable process. Whether it is deliberate elimination symbolized by a mythical creature, a "does/uses" criterion, which singles out a distinctive relationship between two variables, or a hybrid of both, joint doctrine COG determination should be testable. With qualifying standards, COGs are less likely to be misidentified. JFQ

Notes

[1] Joint Publication (JP) 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011), III-23.

[2] On May 14, 2014, the Department of State officially stated that the Islamic State of Iraq and the Levant (ISIL) will be the terrorist organization's primary name. Department of State, "Terrorist Designations of Groups Operating in Syria," available at <www.state.gov/r/pa/prs/ps/2014/05/226067.htm>.

[3] Dale C. Eikmeier, "Redefining the Center of Gravity," *Joint Force Quarterly* 59 (4th Quarter 2010); James P. Butler, "Godzilla Methodology: Means for Determining Center of Gravity," *Joint Force Quarterly* 72 (1st Quarter 2014); Joint Operation Planning Process (JOPP) Workbook, Naval War College Joint Military Operations Department (Newport, RI: U.S. Naval War College, January 21, 2008), appendix C.

[4] "ISIS Rebels Declare "Islamic State" in Iraq and Syria," BBC News, June 30, 2014, available at <www.bbc.com/news/world-middle-east-28082962>; "What is ISIS? The Short Answer," *Wall Street Journal*, June 12, 2014, available at <http://blogs.wsj.com/briefly/2014/06/12/islamic-state-of-iraq-and-al-sham-the-short-answer/>.

[5] Jim Sciutto, Jamie Crawford, and Chelsea J. Carter, "ISIS Can "muster" Between 20,000 and 31,500 Fighters, CIA Says," *CNN.com*, September 12, 2014, available at <www.cnn.com/2014/09/11/world/meast/isis-syria-iraq>.

[6] JP 5-0, III-22.

[7] Eikmeier references that the use of the word *primary* is attributed to Joe Strange, *Centers of Gravity and Critical Vulnerabilities: Building the Clausewitzian Foundation So That We Can All Speak the Same Language*, Perspectives on Warfighting, no. 4, 2nd ed. (Quantico, VA: Marine Corps Association, 1996), ix.

[8] Eikmeier, "Redefining the Center of Gravity."

[9] "Daash Announce the Establishment of the Caliphate State and Renamed the 'Islamic State' Only without Iraq, Syria," *ArabicCNN.com*, June 29, 2014, available at <http://arabic.cnn.com/middleeast/2014/06/29/urgent-isis-declares-caliphate>; Office of the Director of National Intelligence, "Abu

Mohammad, letter dated 9 July 2005,” 2, available at <https://web.archive.org/web/20110522153638/http:/www.dni.gov/press_releases/letter_in_english.pdf>.

[10] Adam Withnall, “Iraq Crisis: ISIS Changes Name and Declares Its Territories a New Islamic State with ‘Restoration of Caliphate’ in Middle East,” *The Independent* (London), June 29, 2014.

[11] Laura Smith-Spark, “Iraqi Yazidi Lawmaker: ‘Hundreds of My People Are Being Slaughtered,’” *CNN.com*, August 6, 2014, available at <http://edition.cnn.com/2014/08/06/world/meast/iraq-crisis-minority-persecution/index.html?hpt=hp_t3>.

[12] Tim Arango and Michael R. Gordon, “Iraqi Insurgents Secure Control of Border Posts,” *New York Times*, June 23, 2014.

[13] Bill Roggio, “The Rump Islamic Emirate of Iraq,” *The Long War Journal*, October 16, 2006, available at <www.longwarjournal.org/archives/2006/10/the_rump_islamic_emi.php>.

[14] Max Fisher, “How ISIS Is Exploiting the Economics of Syria’s Civil War,” *Vox.com*, June 12, 2014, available at <www.vox.com/2014/6/12/5802824/how-isis-is-exploiting-the-economics-of-syrias-civil-war>; Terrence McCoy, “ISIS Just Stole $425 Million, Iraqi Governor Says, and Became the ‘World’s Richest Terrorist Group,’” *Washington Post*, June 12, 2014.

[15] J.M. Berger, “How ISIS Games Twitter,” *The Atlantic*, June 16, 2014, available at <www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/>; Harleen K. Gambhir, Dabiq: *The Strategic Messaging of the Islamic State*, Backgrounder (Washington, DC: Institute for the Study of War, August 15, 2014), available at <www.understandingwar.org/backgrounder/dabiq-strategic-messaging-islamic-state>.

[16] Sciutto, Crawford, and Carter.

[17] ISIL has obtained weapons from Saddam Hussein’s stockpiles, the Syrian civil war, and U.S. involvement in Operation *Iraqi Freedom*. See John Ismay, “Insight into How Insurgents Fought in Iraq,” *New York Times*, October 17, 2013, available at <http://atwar.blogs.nytimes.com/2013/10/17/insight-into-how-insurgents-fought-in-iraq/?_r=1>; Charles Lister, “Not Just Iraq: The Islamic State Is Also on the March in Syria,” *The Huffington Post*, August 7, 2014, available at <www.huffingtonpost.com/charles-lister/not-just-iraq-the-islamic_b_5658048.html?utm_hp_ref=tw>; Thomas Gibbons-Neff, “ISIS Propaganda Videos Show Their Weapons, Skills in Iraq,” *Washington Post*, June 18, 2014, available at <www.washingtonpost.com/news/checkpoint/wp/2014/06/18/isis-propaganda-videos-show-their-weapons-skills-in-iraq/>.

[18] Nick Thompson and Atika Shubert, “The Anatomy of ISIS: How the ‘Islamic State’ Is Run, from Oil to Beheadings,” *CNN.com*, September 18, 2014, available at <http://edition.cnn.com/2014/09/18/world/meast/isis-syria-iraq-hierarchy/index.html?hpt=hp_t1>.

[19] ISIL’s foundation is based on al Qaeda’s ideology and follows well-known jihadist principles. This form of Islam is anti-Western and uses violence against those who do not agree with their views. This branch of Islam seeks to return to original thoughts and condemns new ideas, which are believed to be corrupt. See Michael Glint, *Can a War With ISIS Be Won? ISIL/Islamic State/Daesh* (ebook, Conceptual Kings, 2014), 5; *Violent Extremism Smartcard Compendium*, TRADOC Culture Center first draft, September 2012, 45–52.

[20] “Islamic State: An Assessment of Capabilities and the Effectiveness of International Intervention,” IHS Jane’s Intelligence Briefing, October 30, 2014.

[21] Over the past 6 months, since the group began sweeping across eastern Syria and into Iraq, experts estimate that its leaders have gained access to 1.2 billion pounds in cash—more than the most recent recorded annual military expenditure of Ireland. ISIL is developing in a vital oil, gas, and trade area of the world. It can grab as it expands. It might earn up to 5 million pounds a month through extortion of local businesses. In the past year, it has been estimated that ISIL has made 40 million pounds from taking hostages, with each foreign hostage thought to be worth 3 million pounds. See Harriet Alexander and Alastair Beach, “How ISIL is Funded, Trained and Operating in Iraq and Syria,” *The Telegraph* (London), August 23, 2014, available at <www.telegraph.co.uk/news/worldnews /worldnews/middleeast/iraq/11052919/How-Isil-is-funded-trained-and-operating-in-Iraq-and-Syria.html>.

[22] Eikmeier argued that leaders in World War II were not centers of gravity but were critical requirements as leaders for their respective nations and enablers for the actual centers of gravity. In a modernized military, Eikmeier would not identify soldiers as the operational COG. Depending on the military force, the COG could be armor formations, air forces, or some other component—whichever capability is critical for accomplishing the objectives. See Dale C. Eikmeier, “Center of Gravity Analysis,” *Military Review* (July–August 2004), 2–5.

[23] “ISIS Fast Facts,” *CNN.com*, October 9, 2014, available at <www.cnn.com/2014/08/08/world/isis-fast-facts>.

[24] “Islamic State.”

[25] Ibid.

[26] Butler, 29.

[27] Milan Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: U.S. Naval War College, 2009), VII-16.

[28] Butler, 27.

[29] JOPP Workbook.

[30] “ISIS Fast Facts.”

[31] JOPP Workbook.

[32] “ISIL Brings More than Just Brutality to the Battlefield,” *AmericanAljazeera.com*, November 2, 2014.

[33] Max Abrahms, “What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy,” *International Security* 32, no. 4 (Spring 2008), 97.

[34] Ibid., 104.

Joint Publications (JPs) Under Revision (to be signed within 6 months)

JP 1-0, *Joint Personnel Support*

JP 1-04, *Amphibious Embarkation and Debarkation*

JP 1-06, *Financial Management Support in Joint Operations*

JP 3-05.1, *Unconventional Warfare*

JP 3-13.3, *Operations Security*

JP 3-15, *Barriers, Obstacles, and Mine Warfare*

JP 3-34, *Joint Engineer Operations*

JP 3-50, *Personnel Recovery*

JP 3-61, *Public Affairs*

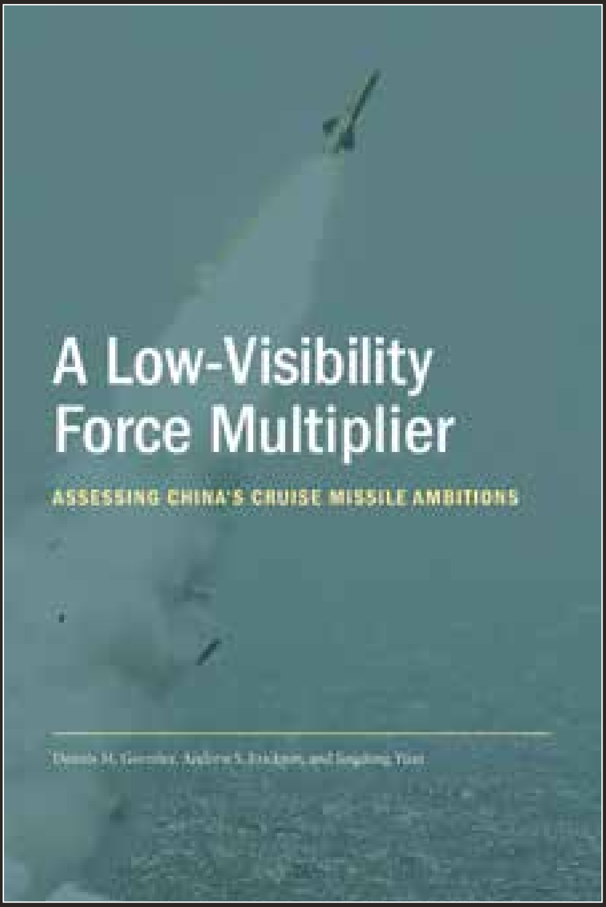
JP 3-68, *Noncombatant Evacuation Operations*

JP 4-01.2, *Sealift Support to Joint Operations*

JP 4-01.5, *Joint Terminal Operations*

JP 4-03, *Joint Bulk Petroleum and Water Doctrine*

JP 6-0, *Joint Communications System*


A Low-Visibility Force Multiplier
ASSESSING CHINA'S CRUISE MISSILE AMBITIONS
Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan

NEW from NDU Press

A Low-Visibility Force Multiplier:
Assessing China's Cruise Missile Ambitions
By Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan

China's military modernization includes ambitious efforts to develop antiaccess/area-denial (A2/AD) capabilities to deter intervention by outside powers. Highly accurate and lethal antiship cruise missiles and land-attack cruise missiles carried by a range of ground, naval, and air platforms are an integral part of this counter-intervention strategy. This comprehensive study combines technical and military analysis with an extensive array of Chinese language sources to analyze the challenges Chinese cruise missiles pose for the U.S. military in the Western Pacific.

"Cruise missiles are key weapons in China's A2/AD arsenal, providing a lethal precision-strike capability against naval ships and land-based targets. The authors use hundreds of Chinese language sources and expertise on cruise missile technology to assess China's progress in acquiring and developing advanced antiship and land-attack cruise missiles and to consider how the People's Liberation Army might employ these weapons in a conflict. Essential reading for those who want to understand the challenges China's military modernization poses to the United States and its allies."

—**David A. Deptula**, Lieutenant General, USAF (Ret.),
Senior Military Scholar, Center for Character and Leadership
Development, U.S. Air Force Academy

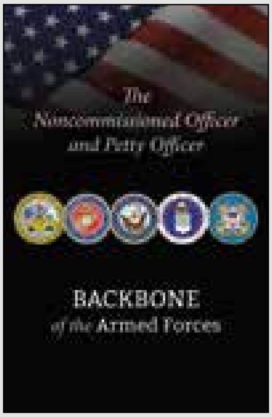
"This volume is a major contribution to our understanding of Chinese military modernization. Although China's ballistic missile programs have garnered considerable attention, the authors remind us that Beijing's investment in cruise missiles may yield equally consequential results."

—**Thomas G. Mahnken**, Jerome E. Levy Chair of
Economic Geography and National Security, U.S. Naval War College

"This book provides an excellent primer on the growing challenge of Chinese cruise missiles. It shows how antiship and land-attack cruise missiles complicate U.S. efforts to counter China's expanding A2/AD capabilities and are becoming a global proliferation threat. The authors also demonstrate just how much progress China has made in modernizing and upgrading its defense industry, to the point of being able to develop and produce world-class offensive weapons systems such as land-attack cruise missiles. This book belongs on the shelves of every serious observer of China's growing military prowess."

—**Richard A. Bitzinger**, Coordinator, Military Transformations Program,
S. Rajaratnam School of International Studies, Singapore

Available online at ndupress.ndu.edu/Portals/68/Documents/Books/force-multiplier.pdf


The Noncommissioned Officer and Petty Officer
BACKBONE of the Armed Forces

The Noncommissioned Officer and Petty Officer: Backbone of the Armed Forces

NDU Press, 2013 • 176 pp.

A first of its kind, this book—of, by, and for noncommissioned officers and petty officers—is a comprehensive explanation of enlisted leaders across the United States Armed Forces. It balances with the Services' NCO/PO leadership manuals and complements *The Armed Forces Officer*, the latest edition of which was published by NDU Press in 2007. Written by a team of Active, Reserve, and retired enlisted leaders from the five Service branches, this book describes how NCOs/POs fit into an organization, centers them in the Profession of Arms, defines their dual roles of complementing the officer and enabling the force, and exposes their international engagement. As Chairman of the Joint Chiefs of Staff General Martin E. Dempsey writes in his foreword to the book, "We know noncommissioned officers and petty officers to have exceptional competence, professional character, and soldierly grit—they are exemplars of our Profession of Arms."

Aspirational and fulfilling, this book helps prepare young men and women who strive to become NCOs/POs, re-inspires currently serving enlisted leaders, and stimulates reflection by those who no longer wear the uniform. It also gives those who have never served a comprehensive understanding of who these exceptional men and women are, and why they are known as the "Backbone of the Armed Forces."

Have you checked out NDU Press online lately?

With 20,000 unique vistors 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